Codes correcteurs avec les polynômes tordus

Lionel Chaussade

N° d'ordre : 4229 ANNÉE 2010

THÈSE / UNIVERSITÉ DE RENNES 1
sous le sceau de l'Université Européenne de Bretagne

pour le grade de

DOCTEUR DE L'UNIVERSITÉ DE RENNES 1

Mention : Mathématiques et Applications

Ecole doctorale Matisse

présentée par

Lionel Chaussade

préparée à l'UMR 6625 CNRS-IRMAR
Institut de Recherche Mathématique de Rennes
U.F.R de Mathématiques

Codes correcteurs avec les polynômes tordus

Thèse soutenue à Rennes le 22 Novembre 2010

devant le jury composé de :

Bruno SALVY
DR INRIA Rocquencourt / rapporteur

Thierry BERGER
Professeur Université Limoges / rapporteur

Pierre LOIDREAU
Chercheur DGA-IM / examinateur

Daniel AUGOT
DR INRIA Rocqencourt / examinateur

Felix ULMER
Professeur Université Rennes / directeur de thèse

Remerciements

J'adresse mes remerciements en premier lieu à mon directeur de thèse, Felix Ulmer ; il a su être présent, m'initier à la beauté de certains objets mathématiques comme les bases de Gröbner et me remotiver durant les périodes creuses de ma thèse. Mon envie de travailler avec Felix a pour origine un cours de licence très vivant sur les groupes qui m'a marqué et a contribué à me faire aimer les objets algébriques. J'ai retrouvé cette passion et cet optimisme lors de nos échanges mathématiques durant ma thèse.

Merci bien évidemment à Thierry Berger et Bruno Salvy qui ont accepté la tâche fastidieuse de relire ma thèse. Leurs remarques ont été précieuses pour faire converger mon manuscrit vers une version plus aboutie. Merci plus particulièrement à Thierry qui m'a accueilli avec bienveillance à Limoges, lorsque je suis venu faire un exposé.

Je salue également la disponibilité de Daniel Augot et Pierre Loidreau qui ont bien voulu compléter mon jury. L'expertise de Pierre dans le domaine des codes correcteurs m'a beaucoup aidé au début de ma thèse à découvrir cette branche des mathématiques avec laquelle je n'étais pas encore familier.

Mes remerciements ne seraient pas complets si j'oubliais Delphine Boucher qui a participé à de nombreuses reprises aux rendez-vous entre Felix et moi. Elle s'est intéressée à ma thèse et a été toujours très disponible lorsque j'avais des questions.

Durant ces trois ans, sortir du cadre du bureau et aller devant des élèves a été comme une bouffée d'air qui m'a permis de prendre du recul sur ma thèse et de m'y replonger avec une nouvelle fraîcheur. Je remercie donc Arnaud Debussche, Michel Pierre, Grégory Vial et Rozenn Texier-Picard qui m'ont accueilli en tant que moniteur à l'ENS de Ker Lann et m'ont permis de dispenser des enseignements très intéressants.

Un grand merci aussi au personnel administratif de l'IRMAR : secrétaires, personnel d'entretien, personnel de la bibliothèque qui contribuent à la bonne ambiance au sein du laboratoire.

Je remercie tous mes amis rennais, déjà 7 ans pour certains que l'on partage tellement de choses ensemble. Que ce soit autour d'un bon et copieux repas, d'un jeu de société, ou

encore sur un cours de tennis, un terrain de foot ou sur une patinoire. Je remercie Clément, Aurélien, Sébastien, Mathilde, Sten, Emilie, Gweltaz et Damian pour leur bonne humeur et leur humour unique. Une pensée également pour mes amis Libournais : Jérôme, Olivier et Guillaume dont les soirées rares mais précieuses passées ensemble ont toujours été très agréables. Merci également à tout ce monde que j'ai croisé durant ma thèse, certains au séminaire de 12h30, d'autres pour nos rendez-vous sportifs du vendredi et bien sûr lors de nos repas traditionnels au RU, je veux parler de Jérémy, Jean-Romain, Victoria, Mikäel, Mouton, Arnaud x2, Viviana, Colas, Richard, Fanny, Pierre, Bachir, Serge, Yao, Delphine, Yann, Sabine, Sandrine, Nirmal, Jon, Maher et j'en oublie très certainement.

Merci à mes parents et à ma soeur pour leur soutien constant ; bien qu'ignorant tout de mon travail mathématique, ils ont su me porter durant ces trois ans en étant constamment aux petits soins avec moi lors de mes séjours à Libourne.

Enfin comment remercier Marie avec qui je partage mon quotidien depuis maintenant plus de 7 ans ; son amour et sa gentillesse ont été comme un phare dans les moments difficiles de ma thèse et je lui dois beaucoup dans l'accomplissement de ce travail.

Table des matières

Liste des algorithmes

Tous les algorithmes et exemples numériques présentés dans cette thèse ont été programmés à l'aide du logiciel de calcul formel Magma (version 2.13). L'intégralité des tableaux exposés dans ce manuscrit sont issus des résultats fournis par ces algorithmes.

Introduction

Cette thèse a pour objet d'étude la théorie des **codes correcteurs**. Ce domaine est relativement récent à l'échelle de l'histoire des mathématiques, il faut remonter en 1948 pour retrouver les prémices de cette théorie dans un article de **Claude Shannon**, le père fondateur de la théorie de l'information. Ses premières idées sont très vite dévoloppées par **Richard Hamming** au début des années 50. Les applications industrielles ont contribué à l'essor rapide de la théorie des codes. En effet, de nos jours, la théorie des codes est omniprésente dans le domaine des communications classiques (radio, fibres optiques) mais également dans les supports de stockage comme les disques compacts où l'intégrité des données est importante.

L'idée à la base de la théorie des codes est simple, un émetteur envoie un message à un récepteur :

$$\begin{array}{ccc} Emetteur & \longrightarrow & But \\ & \uparrow & \\ & Erreurs & \end{array}$$

Des altérations du message pendant le transport peuvent avoir lieu. L'idée de la théorie des codes correcteurs est de transmettre le message initial augmenté d'une **partie redondante** pour détecter et éventuellement corriger des erreurs lors de l'acheminement du message. Un des sujets primordial d'étude est la découverte d'un bon compromis entre la quantité de redondance à ajouter et la capacité de correction ainsi obtenue. Une introduction historique et détaillée de la théorie des codes correcteurs est disponible dans l'ouvrage [22].

La modélisation mathématique de cette théorie est au premier abord assez simple. Etant donné un alphabet $\mathcal{A}$, c'est-à-dire un ensemble de symboles, un code est un sous ensemble de $\mathcal{A}^n$ et ses éléments sont appelés mots. Le lien entre cette modélisation et le problème initial ne sera pas expliqué ici. L'utilisation d'outils algébriques permet d'enrichir cette définition assez simpliste. Par exemple en prenant pour alphabet $\mathcal{A}$ un corps fini $\mathbb{F}$, nous pouvons définir et étudier les sous-espaces vectoriels de $\mathbb{F}^n$ ce sont les **codes linéaires**.

La richesse et la diversité de la théorie des codes vient du fait que l'on peut fabriquer de tels espaces vectoriels à l'aide d'outils algébriques que l'on sait manipuler au préalable. Par exemple les **codes cycliques** sont une famille de codes linéaires construite à l'aide de polynômes à coefficients dans un corps fini et les opérations que l'on sait faire sur les polynômes vont nous donner des renseignements sur la structure du code correcteur. Cette

idée se décline à l'infini, de très nombreux objets algébriques peuvent être exploités pour créer des codes correcteurs. On peut citer par exemple la construction de codes issus de la géométrie algébrique comme les **codes de Goppa** qui utilise en particulier la théorie des variétés sur des corps finis. Il est également possible d'étudier des codes construits à l'aide de graphes.

Dans cette thèse l'outil principal qui sera à l'origine de notre processus de fabrication de codes correcteurs est un anneau polynomial qui a la particularité d'être non-commutatif. Ce type d'anneau a été introduit et étudié largement par Oystein Ore dans l'article « **Theory of Non-commutative Polynomials** » datant de 1933. Plus précisément, si $\mathbb{K}$ est un corps, nous avons de manière ensembliste :

$$\mathbb{K}[X,\theta,\delta] = \{\sum_{i=0}^{n} a_i X^i,\ a_i \in \mathbb{K},\ n \in \mathbb{N}\}.$$

Cet ensemble peut être muni d'une structure d'anneau, l'addition restant celle usuelle sur les polynômes, la multiplication étant définie par la règle suivante :

$$\forall a \in \mathbb{K},\ Xa = \theta(a)X + \delta(a)$$

où θ et δ sont des applications de $\mathbb{K}$ dans $\mathbb{K}$ vérifiant certaines propriétés. Dans toute la suite les objets issus de ce cadre non-commutatif seront parfois qualifiés de « **tordus** », ce sera la traduction française que nous utiliserons de la terminologie anglaise consacrée :« skew ». Cet anneau partage encore de nombreuses propriétés avec $\mathbb{K}[X]$, notamment le fait crucial que ses idéaux à gauche ou à droite sont principaux. Ainsi, une théorie analogue à celle des codes cycliques peut être développée. Cela a été fait dans le cas où $\delta = 0$ par Felix Ulmer, Delphine Boucher et Willy Geiselmann dans les articles [30] et [31]. Dans ces deux articles très récents la méthode de construction des codes correcteurs non-commutatifs est explicitée, une recherche exhaustive de ces codes pour des longueurs raisonnables est présentée, ainsi qu'une étude de la dualité. Il est également à noter qu'une généralisation de ces travaux à des polynômes tordus à coefficients dans un anneau de Galois a été faite par Boucher, Ulmer et Solé dans l'article [8]. La construction de codes correcteurs à l'aide d'anneaux polynomiaux non-commutatifs est en vogue puisque Christophe Chabot dans sa thèse datant de 2010 et dans l'article [3] étudie des codes construits à l'aide d'anneaux de polynômes à coefficients matriciels.

Cette thèse a pour point de départ les articles de Felix Ulmer, Delphine Boucher et Willy Geiselmann. Le **chapitre 1** est une présentation générale des anneaux de Ore ; ceci seront bien sûr étudiés dans l'optique de l'application future à la théorie des codes, en particulier $\mathbb{K}$ sera un corps fini. Nous étudierons les idéaux de ces anneaux tordus avec notamment le théorème 1.4.3 qui affirmera qu'ils sont principaux. Les idéaux bilatères joueront également un rôle particulier puisque l'on demandera que le quotient

$$\mathbb{K}[X,\theta]/I$$

ait une structure d'anneau, ce qui sera le cas lorsque I est un idéal bilatère. Nous nous pencherons également sur la délicate notion de racine d'un polynôme tordu qui nous sera

utile au moment de parler de codes **BCH tordus**. Enfin, une étude brève des dérivations d'un corps fini sera présentée.

Le **chapitre 2** suit essentiellement les deux articles fondateurs mentionnés ci-dessus. Les codes correcteurs tordus y seront définis dans le paragraphe 2.2.2. Plus précisément le polynôme $g = g_0 + g_1X + ... + g_rX^r$ de $\mathbb{K}[X, \theta]$ sera le polynôme générateur du code tordu ayant pour matrice génératrice :

$$\begin{pmatrix} g_0 & \cdots & g_{r-1} & g_r & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \cdots & \theta(g_{r-1}) & \theta(g_r) & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \theta^{n-r-1}(g_0) & \cdots & \theta^{n-r-1}(g_{r-1}) & \theta^{n-r-1}(g_r) \end{pmatrix}.$$

Nous donnerons et commenterons les résultats présentés dans [30] et [31].

Nous obtenons donc une nouvelle famille de codes correcteurs qui contient strictement la famille des codes cycliques. L'intérêt de travailler avec une famille plus large de codes est que l'on a une plus grande latitude, en effet il est possible de faire varier l'automorphisme θ. De plus cet ensemble de codes tordus partage avec les codes cycliques un grand nombre de propriétés, pour résumer, les manipulations polynomiales que nous savons faire dans $\mathbb{K}[X, \theta]$, nous permettrons, comme dans le cas commutatif, d'avoir des résultats sur les codes correcteurs.

Le **chapitre 3** est issu d'un travail en commun avec Felix Ulmer et Pierre Loidreau qui a fait l'objet d'un article : **Skew codes of prescribed distance or rank**. Le but de ce chapitre est de contrôler la distance minimale des codes correcteurs tordus produits à l'aide d'un travail en amont sur le polynôme générateur du code correcteur. Il y a deux aspects abordés dans ce chapitre, le premier concerne la prescription de la distance rang d'un code correcteur ; le théorème qui résume cela est le théorème 3.2.6. Un outil essentiel qui intervient dans cette construction est la théorie des équations aux différences et le lien profond entre ce domaine et la théorie des anneaux de Ore. Cela consiste à associer au polynôme $g = a_0 + a_1X + ... + a_rX^r$ de $\mathbb{K}[X, \theta]$ l'opérateur K^θ-linéaire sur K :

$$L_g(y) = a_0y + a_1\theta(y) + ... + a_r\theta^r(y).$$

Ce type de code correcteur construit à l'aide de la métrique rang a été introduit avec un autre formalisme par Gabidulin dans [9]. Les codes que l'on obtient ici forment toutefois une famille plus vaste que celle présentée par Gabidulin. Le second aspect développé dans ce chapitre est la construction de codes BCH tordus. Les codes BCH introduits par Bose, Ray-Chaudhuri et Hocquenghem sont des codes cycliques dont on peut minorer la distance minimale si l'on a des informations sur les racines du polynôme générateur. Le paragraphe 3.3.2 présente la généralisation des codes BCH à ce contexte non-commutatif. Des algorithmes explicites peuvent être déduits de ces études, c'est ainsi que nous avons trouvé deux codes correcteurs, l'un de paramètres $[42, 14, 21]$ sur $\mathbb{F}_8$ issu de la construction à l'aide de la métrique rang et l'autre de paramètres $[40, 23, 10]$ sur $\mathbb{F}_4$ qui est un code BCH tordu. Ces codes améliorent de 1 la meilleure distance minimale connue pour ces longueurs et dimensions. Enfin, un algorithme de décodage des codes BCH tordu sera présenté.

Le **chapitre 4** présente une généralisation des codes tordus vus précédemment. Son point de départ est l'article [29]. En utilisant le langage des modules, il est possible de s'affranchir des questions tournant autour des idéaux bilatères, en effet si I est un idéal à gauche de $\mathbb{K}[X,\theta]$ alors le quotient $\mathbb{K}[X,\theta]/I$ n'a pas, a priori, une structure d'anneau mais c'est au moins un $\mathbb{K}[X,\theta]$-module. Cela s'avère suffisant pour construire nos codes correcteurs tordus. Nous obtiendrons alors une famille de codes issus d'idéaux polynomiaux encore strictement plus vaste. Un des intérêts de cette approche sera qu'il va être plus accessible d'introduire une dérivation δ à notre anneau de polynômes non-commutatifs et d'étudier les codes qui en résultent. Nous parlerons brièvement des conséquences qu'a cette généralisation sur le chapitre précédent, cette relaxation permettra d'alléger la procédure de calcul et de trouver de nouveaux codes correcteurs ayant une distance minimale record, comme le code présenté dans l'exemple 4.4.3.

Le **chapitre 5** passe dans le monde multivarié. Ce sujet a fait l'objet d'une prépublication IRMAR sous le titre : **Codes on multivariate Ore polynomial rings**. L'idée principale est d'étudier des codes correcteurs vus comme quotients d'anneaux non-commutatifs de polynômes à plusieurs variables par un idéal bilatère. L'écueil majeur est le fait que les idéaux que l'on va étudier ne sont plus principaux. Un travail préalable sur les idéaux en utilisant les bases de Gröbner sera donc un passage obligatoire. Il faudra légèrement adapter l'algorithme de Buchberger dans ce cadre. Le paragraphe 5.3 montrera que l'on peut prévoir la dimension de ces codes et obtenir au prix de quelques divisions polynomiales la matrice génératrice sous forme systématique. Un des avantages de cet univers multivarié est que l'on va avoir une liberté supplémentaire sur nos paramètres. En effet, en une variable, une fois choisi le polynôme générateur et la longueur du code, le code est fixé, tandis qu'en plusieurs variables nous pouvons jouer sur la forme de l'escalier des idéaux avec lesquels on va travailler. Tout ceci sera précisé dans le paragraphe 5.5.

Il reste encore de nombreuses questions à étudier autour de ces familles de codes correcteurs tordus, en particulier des questions de stabilité des codes modules par un automorphisme monomial. Une première approche sera expliquée brièvement dans le chapitre perspectives et on présentera notamment un algorithme permettant de tester si un code correcteur est un code-module. On peut également envisager une généralisation supplémentaire en introduisant des anneaux non-commutatifs multivariés différents.

Notations et notions de base

Représentations des corps finis

L'entier p désignera un nombre premier et l'on travaillera très souvent avec le corps fini à $q = p^t$ éléments que l'on notera $\mathbb{F}_q$. L'anneau des polynômes à une indéterminée sur un corps $\mathbb{K}$ sera noté $\mathbb{K}[\mathbb{X}]$.

La construction suivante est légitimée par le fait qu'il existe au moins un polynôme irréductible de $\mathbb{F}_p[X]$ de degré t.

Soit $P \in \mathbb{F}_p[X]$ de degré t irréductible, nous avons l'isomorphisme de corps :

$$\mathbb{F}_q \simeq \mathbb{F}_p[X]/\langle P \rangle.$$

Pour manipuler les éléments de $\mathbb{F}_q$, nous nous servirons de cette correspondance et travaillerons dans le quotient $\mathbb{F}_p[X]/\langle P \rangle$ en notant $\alpha = \overline{X}$. Pour chaque paramètre n et t, il est possible de choisir P afin que α engendre le groupe des inversibles de $\mathbb{F}_q$, que nous notons $\mathbb{F}_q^*$. Cette propriété est démontrée au chapitre 2 de [14].

Dans la suite, nous choisirons P de cette manière là et nous exprimerons les éléments de $\mathbb{F}_q$ sous la forme de puissance de α. Le polynôme P sera celui donné par le logiciel de calcul formel Magma. dans sa version 2.13.

Voici une liste des polynômes P utilisés pour $p = 2$ et $p = 3$ qui sont les principales caractéristiques que nous utiliserons. Il sont donnés par la commande ConwayPolynomial(p,t) du logiciel de calcul formel Magma.

	$p = 2$	$p = 3$
$t = 2$	$X^2 + X + 1$	$X^2 + 2X + 2$
$t = 3$	$X^3 + X + 1$	$X^3 + 2X + 1$
$t = 4$	$X^4 + X + 1$	$X^4 + 2X^3 + 2$
$t = 5$	$X^5 + X^2 + 1$	$X^5 + 2X + 1$
$t = 6$	$X^6 + X^4 + X^3 + X^2 + X + 1$	$X^6 + 2X^4 + X^2 + 2X + 2$

Nous noterons par la suite, même lorsque ce n'est pas précisé, α le générateur de $\mathbb{F}_q^*$ donné par Magma dans sa version 2.13.

Automorphismes de $\mathbb{F}_q$

Soit $q = p^t$ où p est un nombre premier, on notera $\theta(x) = x^p$, l'automorphisme de Frobenius.

Cet automorphisme particulier engendre le groupe des automorphismes de $\mathbb{F}_q$ puisque :
Théorème. — *Le groupe des automorphismes de $\mathbb{F}_q$ est cyclique d'ordre t engendré par l'automorphisme de Frobenius :*

$$Aut(\mathbb{F}_q) = \{Id,\ x \mapsto x^p,\ x \mapsto x^{p^2},\ ...,\ x \mapsto x^{p^{r-1}}\}.$$

Cela est démontré, par exemple, dans le théorème 2.21 de [14].

Notation 1. — L'écriture θ^i désignera la composée de θ i-fois.

Notation 2. — Dans la suite, nous noterons $(\mathbb{F}_q)^\theta$ le sous-corps de $\mathbb{F}_q$ fixé par l'automorphisme θ.

Rappels sur les codes correcteurs

Dans cette thèse, nous étudierons uniquement des codes correcteurs linéaires et l'alphabet sera un corps fini, c'est ce qui sera sous-entendu dans la suite par "code". Nous appellerons mot de code un élément du code.
Définition. — *Un code de longueur n et de dimension k est un sous $\mathbb{F}_q$-espace vectoriel de $\mathbb{F}_q^n$ de dimension k.*

On note $M_{k,n}(\mathbb{F}_q)$, l'ensemble des matrices à k lignes et n colonnes à coefficients dans $\mathbb{F}_q$.

Définition. — *Une matrice génératrice d'un code de longueur n et de dimension k est une matrice de $M_{k,n}(\mathbb{F}_q)$ dont les lignes forment une base de ce code.*

Définition. — *Une matrice de parité d'un code, $\mathcal{C}$, est une matrice $H \in M_{n-k,n}(\mathbb{F}_q)$, telle que pour tout $c \in \mathcal{C}$:*

$$H^t c = 0.$$

Définition. — *Le poids de Hamming d'un mot $c = (c_1, ..., c_n) \in \mathcal{C}$, noté $\omega(c)$, est défini par :*

$$\omega(c) = \sharp\{i,\ c_i \neq 0\}.$$

Définition. — *La distance de Hamming d'un code $\mathcal{C}$, notée $d(\mathcal{C})$, est définie par :*

$$d(\mathcal{C}) = \min_{x \in \mathcal{C},\ x \neq 0} \{\omega(x)\}.$$

On parlera d'un code de paramètres $[n, k, d]$ pour désigner un code de longueur n, de dimension k et de distance minimale d. Nous rappelons que la borne de Singleton affirme que $k \leq n + 1 - d$.

Pour une introduction élémentaire, on pourra consulter [32].

Chapitre 1

Anneaux de Ore sur un corps fini

1.1 Motivation

Il existe de très nombreuses façons de construire un code correcteur, l'une d'entre elles consiste à utiliser un anneau de polynômes. Plus précisément, on considère l'anneau $\mathbb{F}_q[X]$. C'est un anneau euclidien et en particulier principal. Nous pouvons choisir un entier n et regarder l'anneau quotient $\mathbb{F}_q[X]/\langle X^n-1\rangle$, l'application fondamentale qui va nous permettre d'associer un polynôme à un mot de code est la suivante :

$$\begin{array}{rccc} T & : & \mathbb{F}_q^n & \to & \mathbb{F}_q[X]/\langle X^n-1\rangle \\ & & (a_0,a_1,...,a_{n-1}) & \mapsto & a_0+a_1X+...+a_{n-1}X^{n-1}. \end{array}$$

Nous avons la définition d'un code **cyclique** :

Définition. — *Un code cyclique est l'image réciproque par T d'un idéal de $\mathbb{F}_q[X]/\langle X^n-1\rangle$.*

Les idéaux de $\mathbb{F}_q[X]/\langle X^n-1\rangle$ sont connus puisqu'ils sont en correspondance avec les diviseurs dans $\mathbb{F}_q$ de X^n-1.

Cette construction et ses propriétés seront détaillées au chapitre 2.

En résumé les points cruciaux de cette construction sont :

1. L'analogie mots de code et polynômes via l'application T.
2. Le caractère euclidien de l'anneau $\mathbb{F}_q[X]$ afin de pouvoir travailler facilement dans des quotients de cet anneau.
3. La connaissance des idéaux de $\mathbb{F}_q[X]$ qui sont principaux.
4. L'étude des diviseurs de X^n-1 dans $\mathbb{F}_q[X]$.

Le point de départ de cette thèse est de mettre au point une construction analogue à celle là avec un anneau de polynômes non-commutatif.

L'exemple d'anneau non-commutatif que nous allons utiliser au début est le suivant :

$$\mathbb{F}_q[X,\theta]=\{\sum_{i=0}^{m}a_iX^i,\ a_i\in\mathbb{F}_q,\ m\in\mathbb{N}\}. \tag{1.1}$$

L'addition est l'addition usuelle et la multiplication est définie en étendant par associativité et distributivité la règle :

$$\forall \boldsymbol{a} \in \mathbb{F}_{\boldsymbol{q}},\ \boldsymbol{Xa} = \boldsymbol{\theta(a)X}. \tag{1.2}$$

Tous les détails de cette construction seront donnés au paragraphe 2 du chapitre 1.

Il faut se demander si la construction que l'on a faite dans le cadre commutatif s'adapte facilement au cadre non-commutatif.

Nous allons reprendre l'énumération des quatre points fondamentaux de cette construction et examiner s'ils s'adaptent en non-commutatif.

1. L'application de passage entre les mots du codes et les polynômes tordus reste bien définie comme en commutatif.
2. Il sera montré dans le paragraphe 2 du chapitre 1 que l'anneau $\mathbb{F}_q[X, \theta]$ est euclidien à gauche et à droite, quitte à bien choisir au préalable le sens dans lequel on divise, il est donc tout à fait possible d'effectuer des divisions euclidiennes.
3. Les idéaux de $\mathbb{F}_q[X, \theta]$ seront examinés au paragraphe 3 du chapitre 1, et l'on verra que là aussi il convient de faire la distinction entre idéaux à droite et à gauche.
4. Enfin l'étude des diviseurs de $X^n - 1$ dans l'anneau $\mathbb{F}_q[X, \theta]$ va être particulièrement intéressante afin de pouvoir dénombrer les codes que l'on va obtenir. En effet, nous allons voir au paragraphe 5 du chapitre 1 que la factorisation dans l'anneau $\mathbb{F}_q[X, \theta]$ est plus complexe qu'en commutatif.

Une difficulté supplémentaire apparaît en non-commutatif ; lorsque l'on quotiente $\mathbb{F}_q[X, \theta]$ par un idéal, le quotient a une structure d'anneau uniquement lorsque l'idéal est bilatère.

Il sera naturel d'étudier la structure des idéaux bilatères de $\mathbb{F}_q[X, \theta]$, cette question sera abordée également dans le chapitre 1.

Nous voyons qu'il faut dans un premier temps étudier attentivement la structure de $\mathbb{F}_q[X, \theta]$ afin de pouvoir construire, par analogie aux codes cycliques, des codes θ-cycliques.

Le chapitre 1, dont nous allons à présent détailler le sommaire, va être entièrement consacré à cette étude.

Le but de ce chapitre est d'introduire et de regarder les propriétés d'une famille d'anneaux de polynômes non-commutatifs. Ce type d'anneau a été introduit et étudié par Ore en 1933 dans [21]. Cette étude a été poursuivie par Jacobson dans l'ouvrage [13] et [12]. Le livre de Cohn [5] en fait également largement mention.

Dans cette partie, nous allons développer les propriétés de ces anneaux qui vont nous servir dans la construction des codes que l'on va effectuer plus tard, en particulier les textes de Ore et Jacobson considèrent ces anneaux de polynômes sur un corps quelconque tandis que nous allons étudier ici la théorie uniquement sur un corps fini. Il faut garder à l'esprit qu'une grande partie des résultats évoqués sont encore vrais sur d'autres corps. En ce qui concerne le cas des anneaux de polynômes non-commutatifs à coefficients dans un anneau voir [33].

Nous allons voir dans un premier temps la définition ainsi que les premières propriétés de ces anneaux, nous remarquerons en particulier que la famille d'anneaux considérée est vaste puisque ces anneaux ne sont pas isomorphes entre eux. Puis, nous mettrons en évidence le caractère euclidien à gauche et à droite, ce résultat fondamental résumé dans le théorème 1.3.1 sera un des ingrédients principaux pour parler de codes correcteurs. Nous étudierons également les idéaux de cet anneau qui, à cause de la non-commutativité, seront des idéaux à gauche ou à droite. Bien entendu, les idéaux bilatères joueront un rôle particulièrement intéressant, ils seront caractérisés dans le théorème 1.4.5. Nous regarderons également le centre de cet anneau de polynômes non-commutatif et nous définirons la notion de borne d'un polynôme. Le théorème 1.5.4, nous dira que tout polynôme possède une borne, c'est-à-dire un multiple qui est central. Puis nous nous intéresserons aux propriétés arithmétiques de ces anneaux, notamment à des problèmes de factorisation et d'irréductibilité, avec la définition d'une racine d'un polynôme tordu. Le théorème 1.7.14 permettra de quantifier le défaut de factorialité de ces anneaux. Enfin le dernier paragraphe généralisera encore nos anneaux en introduisant une dérivation compliquant un peu plus la multiplication de deux polynômes tordus. A cet effet, nous caractériserons les dérivations d'un corps fini.

1.2 Définition et généralités

Dans ce chapitre, nous allons définir l'anneau non-commutatif en question, puis étudier ses premières propriétés et voir un exemple de calcul.

Soit p un nombre premier et $t \in \mathbb{N}^*$. On note $\mathbb{F}_q$ le corps fini à q éléments où $q = p^t$. Soit θ un automorphisme de corps de $\mathbb{F}_q$. On définit l'ensemble suivant :

$$\mathbb{F}_q[X, \theta] = \{\sum_{i=0}^{m} a_i X^i,\ a_i \in \mathbb{F}_q,\ m \in \mathbb{N}\}. \tag{1.3}$$

On va munir cet ensemble d'une structure d'anneau. On garde l'addition usuelle sur les polynômes. La multiplication va être définie par la règle simple :

$$\boldsymbol{\forall a \in \mathbb{F}_q,\ Xa = \theta(a)X.} \tag{1.4}$$

En étendant cette règle par associativité et distributivité, on obtient une loi de multiplication bien définie sur $\mathbb{F}_q[X, \theta]$. En effet de manière plus générale si :

$$P = \sum_{i=0}^{m} a_i X^i$$

et

$$Q = \sum_{i=0}^{n} b_j X^j$$

on peut effectuer le produit PQ et l'on obtient en distribuant :

$$PQ = \sum_{i,j} a_i X^i b_j X^j.$$

Il suffit de remarquer que $X^i b_j = \theta^i(b_j)X^i$ en itérant la règle de multiplication (1.4). Au final, on a :

$$PQ = \sum_{i,j} a_i \theta^i(b_j) X^{i+j}.$$

Remarque 1.2.1. — Le fait de demander que θ soit un automorphisme de corps est une condition assez naturelle. En effet, on a envie d'avoir les propriétés suivantes :

$$X(a+b) = Xa + Xb$$

$$X(ab) = (Xa)b$$

$$X1 = X.$$

Ces trois propriétés reviennent à demander respectivement que θ soit un morphisme additif, multiplicatif et unitaire.

Remarque 1.2.2. — On retrouve l'anneau classique de polynômes à coefficients dans un corps fini lorsque l'automorphisme θ est égal à l'identité ; c'est-à-dire $\mathbb{F}_q[X, Id] = \mathbb{F}_q[X]$. Cependant, il est clair que si l'automorphisme que l'on choisit est distinct de l'identité, on obtient un anneau de polynômes non-commutatif, aussi appelé anneau de polynômes tordus.

Exemple 1.2.3. — Afin d'avoir à notre disposition un automorphisme de corps non trivial, il convient de se placer dans un corps de cardinal non premier. Prenons $\mathbb{F}_4$ et l'automorphisme $\theta(x) = x^2$. Pour faciliter les calculs dans $\mathbb{F}_4$, on voit ce corps comme étant $\mathbb{F}_2[X]/\langle X^2 + X + 1\rangle$. En notant $\alpha = \bar{X}$, on a $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, avec la relation fondamentale $\alpha^2 = \alpha + 1$. Soit $P = X^2 + \alpha X \in \mathbb{F}_q[X, \theta]$ et $Q = \alpha^2 X + 1 \in \mathbb{F}_q[X, \theta]$, on a alors :

$$\begin{aligned} PQ &= (X^2 + \alpha X)(\alpha^2 X + 1) \\ &= X^2\alpha^2 X + \alpha X \alpha^2 X + X^2 + \alpha X \\ &= \theta^2(\alpha^2)X^3 + \alpha\theta(\alpha^2)X^2 + X^2 + \alpha X \\ &= \alpha^2 X^3 + \alpha^2 X^2 + X^2 + \alpha X \\ &= \alpha^2 X^3 + \alpha X^2 + \alpha X. \end{aligned}$$

Voyons à présent les premières propriétés de cet anneau.

Définition 1.2.4. — *On définit, de manière analogue au cas commutatif, le* ***degré*** *de* $P = \sum a_i X^i \in \mathbb{F}_q[X, \theta]$ *comme étant le* $\max\{i \in \mathbb{N},\ a_i \neq 0\}$. *On le note* $\deg(P)$. *On adopte la convention* $\deg(0) = -\infty$.

Nous avons également les mêmes propriétés que dans le cas commutatif :

Proposition 1.2.5. — *Soit* P *et* Q *appartenant à* $\mathbb{F}_q[X, \theta]$, *non nuls.*

(i) $\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\}$.
(ii) $\deg(PQ) = \deg(P) + \deg(Q)$.

Démonstration. — La première formule est évidente, l'addition sur les polynômes tordus étant la même que dans le cas commutatif. La seconde assertion provient du fait que $\mathbb{F}_q$ est intègre et que θ est un automorphisme de corps. ∎

Proposition 1.2.6. — *L'anneau $\mathbb{F}_q[X, \theta]$ est intègre et ses inversibles sont exactement les inversibles de $\mathbb{F}_q$.*

Démonstration. — L'outil du degré, introduit précédemment, permet de montrer ces deux assertions immédiatement. ∎

La famille d'anneaux non-commutatifs que l'on obtient est assez grande en effet :

Théorème 1.2.7. — *Les anneaux $\mathbb{F}_{q_1}[X, \theta_1]$ et $\mathbb{F}_{q_2}[Y, \theta_2]$ sont isomorphes si et seulement si $q_1 = q_2$ et $\theta_1 = \theta_2$.*

Démonstration. — Supposons les deux anneaux isomorphes, ils doivent avoir le même nombre d'inversibles, ceci impose $q_1 = q_2$. Notons φ cet isomorphisme, on remarque que $\varphi(\mathbb{F}_{q_1}) = \mathbb{F}_{q_2}$. En effet si tel n'etait pas le cas l'image d'un élément non trivial de $\mathbb{F}_{q_1}$ serait de degré non nul ainsi les images des puissances de cet élément seraient de degré arbitrairement grand ce qui est absurde. Donc φ restreint à $\mathbb{F}_q$ ($q = q_1 = q_2$) est un isomorphisme. Observons que $\varphi(X)$ est de degré 1, car sinon Y n'aurait pas d'antécédent par φ. Posons $\varphi(X) = aY + b$. On a :

$$\varphi(X\alpha) = \varphi(X)\varphi(\alpha) = (aY + b)\varphi(\alpha) = a\theta_2(\varphi(\alpha))Y + b\varphi(\alpha) \tag{1.5}$$

et d'autre part :

$$\varphi(X\alpha) = \varphi(\theta_1(\alpha)X) = \varphi(\theta_1(\alpha))aY + \varphi(\theta_1(\alpha))b. \tag{1.6}$$

Si $b \neq 0$, en regardant les termes constants de (1.5) et (1.6), on voit que cela impose $\theta_1(\alpha) = \alpha$ puisque φ est un isomorphisme de $\mathbb{F}_q$. Un anneau commutatif ne pouvant être isomorphe à un anneau non-commutatif cela impose que $\theta_2 = \theta_1 = Id$. Sinon, si $b = 0$, on a $\theta_2(\varphi(\alpha)) = \varphi(\theta_1(\alpha))$. Toutes les applications mises en jeu font partie du groupe des automorphismes de $\mathbb{F}_q$ qui est commutatif donc $\theta_1 = \theta_2$, ce qui démontre le résultat. ∎

1.3 Division euclidienne

Nous allons à présent voir, de manière identique au cas commutatif, qu'il est possible d'effectuer des divisions euclidiennes. Toutefois, il faudra faire évidemment attention de quel côté on divise à cause de la non-commutativité. Ce processus est détaillé dans [21] dans un cadre très général. Le cas des corps finis est traité dans [16]. Le théorème suivant est crucial puisque le fait de pouvoir diviser permettra plus tard de considérer des anneaux quotients et d'aboutir à la construction de codes correcteurs. Plus précisément, on a le résultat suivant qui est une division euclidienne à droite :

Théorème 1.3.1. — *Soient f et g dans $\mathbb{F}_q[X,\theta]$ avec $g \neq 0$, alors il existe q et r dans $\mathbb{F}_q[X,\theta]$ tels que :*

$$f = qg + r$$

et

$$\deg(r) < \deg(g).$$

Démonstration. — Si $\deg(f) < \deg(g)$, il suffit de prendre $q = 0$ et $r = f$. Supposons donc que $\deg(f) \geq \deg(g)$. On note :

$$f = a_0 + a_1X + ... + a_nX^n$$

$$g = b_0 + b_1X + ... + b_mX^m$$

avec $n \geq m$. L'idée va être de voir qu'à l'aide du terme dominant de g on peut éliminer le terme dominant de f. En effet le polynôme :

$$f - a_n\theta^{n-m}(b_m^{-1})X^{n-m}g$$

est de degré au plus $n-1$ puisqu'il est précisément construit pour faire s'annuler les termes dominants. On poursuit le processus par récurrence. ∎

Remarque 1.3.2. — Il y a également unicité du quotient et du reste.

Remarque 1.3.3. —Il est possible d'obtenir le même résultat en effectuant la division à gauche. En gardant les mêmes notations que dans la preuve précédente, on a :

$$f - g\theta^{-m}(\frac{a_n}{b_m})X^{n-m}$$

qui est de degré au plus $n-1$. Donc, il existe q_1 et r_1 avec $\deg(r_1) < \deg(g)$ tels que :

$$f = gq_1 + r_1.$$

Exemple 1.3.4. — On se place toujours dans $\mathbb{F}_4[X,\theta]$ où $\theta(x) = x^2$. Soient :

$$f = \alpha X^2 + X + \alpha^2$$

$$g = \alpha X + 1.$$

Le résultat de la division à droite est :

$$\alpha X^2 + X + \alpha^2 = (\alpha^2 X + 1)(\alpha X + 1) + \alpha.$$

Le résultat de la division à gauche est :

$$\alpha X^2 + X + \alpha^2 = (\alpha X + 1)X + \alpha^2.$$

L'existence de cet outil de division euclidienne va être fondamentale par la suite. Nous venons de démontrer que :

Théorème 1.3.5. — *L'anneau $\mathbb{F}_q[X,\theta]$ est* ***euclidien à droite et à gauche****.*

Remarque 1.3.6. — En particulier, il faut garder à l'esprit qu'il est tout à fait possible d'utiliser l'algorithme d'Euclide pour calculer un pgcd ou un ppcm en ayant au préalable choisi le côté de division. Les notions de pgcd à gauche et à droite et de ppcm à gauche et à droite sont bien définies.

1.4 Les idéaux de $\mathbb{F}_q[X,\theta]$

Nous allons dans ce paragraphe étudier la structure des idéaux de cet anneau. Plus précisément, nous allons caractériser les idéaux bilatères dans le théorème 1.4.5.
Notation 3. — On notera $\langle P\rangle_g$ l'idéal à gauche engendré par le polynôme P et de même $\langle P\rangle_d$ pour l'idéal à droite. En l'absence de précisions $\langle P\rangle$ désignera l'idéal engendré à gauche par P.

Tout d'abord une conséquence immédiate du paragraphe précédent :

Proposition 1.4.1. — *Tout idéal à gauche de $\mathbb{F}_q[X,\theta]$ est **principal**.*

Démonstration. — Soit I un idéal à gauche non réduit au polynôme nul. On choisit un polynôme non nul de plus bas degré dans I, notons le g. Soit $f \in I$, effectuons la division euclidienne à droite de f par g :

$$f = qg + r$$

avec $\deg(r) < \deg(g)$ ou $r = 0$. On remarque que $r = f - qg$ est dans l'idéal I, comme on avait pris g de degré minimal dans I cela implique que $r = 0$. Donc tout élément de I est un multiple à gauche de g. Le polynôme g engendre à gauche l'idéal I. ∎

Remarque 1.4.2. – De manière similaire, en utilisant la division euclidienne à gauche, on montre que tout idéal à droite est principal.

Nous avons donc démontré le résultat suivant :

Théorème 1.4.3. — *L'anneau $\mathbb{F}_q[X,\theta]$ est principal à droite et à gauche.*

Nous allons à présent déterminer la forme générale des idéaux bilatères de $\mathbb{F}_q[X,\theta]$. On va avoir besoin du lemme intermédiaire suivant :

Lemme 1.4.4. — *Soit I un idéal bilatère de $\mathbb{F}_q[X,\theta]$, alors tout générateur à gauche de I est également un générateur à droite.*

Démonstration. — En tant qu'idéal à gauche, on a l'existence de f tel que $I = f\mathbb{F}_q[X,\theta]$ et en tant qu'idéal à droite on a l'existence de g tel que $I = \mathbb{F}_q[X,\theta]g$. Il existe donc s et t dans $\mathbb{F}_q[X,\theta]$ tels que $fs = g$ et $tg = f$. Le polynôme tf est dans I, donc $tf = ft'$ pour un certain t'. On obtient :

$$f = tg = tfs = ft's. \tag{1.7}$$

Grâce à (1.7), on voit que $t's = 1$ et que s est inversible, ce qui montre que f génère l'idéal à droite également. Evidemment la réciproque est vraie, tout générateur à droite est un générateur à gauche. ∎

A présent, on peut donner la forme des polynômes qui génèrent un idéal bilatère.

Théorème 1.4.5. — *Si f génère un idéal bilatère alors f est de la forme :*

$$(a_0 + a_1X^s + ... + a_nX^{ns})X^p$$

où $s = | < \theta > |$ est l'ordre de θ.

Démonstration. — Soit f un générateur d'un idéal bilatère I non nul, que l'on écrit sous la forme :

$$f = a_0X^p + a_1X^{p+1} + ... + a_nX^{p+n}$$

avec p choisi de telle sorte que a_0 soit non nul. Il est immédiat de voir que X^p génère un idéal bilatère de $\mathbb{F}_q[X, \theta]$, par conséquent $a_0 + a_1X + ... + a_nX^n$ génère également un idéal bilatère qui est juste obtenu en divisant tous les polynômes de I par X^p. On peut donc supposer que

$$f = a_0 + a_1X + ... + a_nX^n$$

où $a_0 \neq 0$. Soit $\beta \in \mathbb{F}_q$, d'après le lemme 1.4.4 , il existe δ tel que $\beta f = f\delta$, c'est-à-dire :

$$a_0\beta + a_1\beta X + ... + a_n\beta X^n = a_0\delta + a_1\theta(\delta)X + ... + a_n\theta^n(\delta)X^n.$$

Ceci en tenant compte que, pour une raison de degré, δ est une constante. Par identification, on a :

$$\beta = \delta,\ a_1\beta = a_1\theta(\delta), ...,\ a_n\beta = a_n\theta^n(\delta).$$

Donc si $a_i \neq 0$ alors i est un multiple de l'ordre de θ, c'est-à-dire :

$$f = \alpha_0 + \alpha_1X^s + ... + \alpha_mX^{ms}.$$

■

Les polynômes du centre de $\mathbb{F}_q[X, \theta]$ engendrent bien entendu des idéaux bilatères. Ces idéaux bilatères particuliers joueront un rôle crucial par la suite. On va par conséquent étudier le centre de $\mathbb{F}_q[X, \theta]$.

Théorème 1.4.6. — *Le centre de $\mathbb{F}_q[X, \theta]$ est $(\mathbb{F}_q)^\theta[X^s]$ où s est l'ordre de θ dans le groupe des automorphismes de $\mathbb{F}_q$ et $(\mathbb{F}_q)^\theta$ désigne le corps des éléments laissés fixes par θ.*

Démonstration. — Par linéarité, il suffit de traduire la condition de commutation avec les constantes et la condition de commutation avec l'indéterminée X. Soit un polynôme du centre de $\mathbb{F}_q[X, \theta]$:

$$f = a_0 + a_1X + ... + a_nX^n.$$

Alors pour tout $\alpha \in \mathbb{F}_q$, on a $\alpha f = f\alpha$ ce qui se traduit par :

$$\alpha a_0 + \alpha a_1X + ... + \alpha a_nX^n = a_0\alpha + a_1\theta(\alpha)X + ... + a_n\theta^n(\alpha)X^n.$$

Comme dans la preuve précédente, on conclut que seules les puissances de X multiples de s apparaissent dans f. D'autre part la condition $Xf = fX$ se traduit par :

$$\theta(a_0)X + \theta(a_1)X^2 + ... + \theta(a_n)X^{n+1} = a_0X + a_1X^2 + ... + a_nX^{n+1}.$$

Ceci signifie que pour tout i, on a $a_i \in (\mathbb{F}_q)^\theta$. Ce qui achève la caractérisation des éléments centraux. ■

1.5 Borne d'un polynôme

Dans ce paragraphe nous allons répondre à la question simple suivante mais qui sera cruciale pour notre construction de codes correcteurs : un polynôme $P \in \mathbb{F}_q[X, \theta]$ a t-il toujours un multiple central ? Le théorème 1.5.4 répond par l'affirmative à cette question et nous donne un algorithme pour calculer ce multiple central, ainsi qu'une majoration de son degré.

Définition 1.5.1. — *Soit $P \in \mathbb{F}_q[X, \theta]$, on dit que P est borné si l'idéal à gauche $\langle P \rangle_g$ contient un idéal bilatère non trivial $\langle P^* \rangle$. Le polynôme P^* unitaire de degré minimal satisfaisant cette condition est appelé* ***borne*** *de P.*

Définition 1.5.2. — *Avec les mêmes notations, on suppose que $\langle P \rangle_g$ contient $\langle P^{**} \rangle$ où P^{**} est central. Le P^{**} unitaire de degré minimal vérifiant cette condition est appelé* ***borne centrale*** *de P.*

Remarque 1.5.3. — Ces conditions reviennent à demander que P^* et P^{**} soient des multiples à gauche de P.

Montrons que P possède toujours une borne et même une borne centrale. On peut en outre contrôler le degré de ces bornes et l'on dispose d'un moyen algorithmique rapide de les calculer.

Théorème 1.5.4. — *Soit $s = |<\theta>|$ et $d = [\mathbb{F}_q : (\mathbb{F}_q)^\theta]$. Soit $P \in \mathbb{F}_q$ de degré n, il existe une borne P^* et une borne centrale P^{**} telles que* $\mathbf{deg(P^*) \leq sn}$ *et* $\mathbf{deg(P^{**}) \leq snd}$ *.*

Démonstration. — On considère les divisions euclidiennes à droite suivantes :

$$X^{is} = Q_i P + R_i, \ i = 0, 1, ..., n \tag{1.8}$$

avec $\deg(R_i) < n$. La famille $\{R_i, \ i = 0...n\}$ fait partie de l'espace vectoriel $\mathbb{F}_q[X, \theta]_{n-1}$ des polynômes à coefficients dans $\mathbb{F}_q[X, \theta]$ de degré plus petit ou égal à $n-1$ qui est de dimension n sur $\mathbb{F}_q$. Il existe une combinaison linéaire non triviale :

$$\sum_{i=0}^{n} \delta_i R_i, \ \delta_i \in \mathbb{F}_q.$$

En effectuant la même combinaison linéaire sur les égalités (1.8), on obtient :

$$\sum_{i=0}^{n} \delta_i X^{is} = (\sum_{i=0}^{n} \delta_i Q_i) P.$$

Le polynôme P est un diviseur à droite de $\sum_{i=0}^{n} \delta_i X^{is}$ qui génère bien un idéal bilatère d'après le théorème 3.5. C'est donc une borne pour P et son degré est plus petit que sn. Pour la seconde assertion du théorème, on remarque que $\mathbb{F}_q[X, \theta]_{n-1}$ est également un espace vectoriel de dimension finie nd sur $(\mathbb{F}_q)^\theta$. En effet $\mathbb{F}_q$ est une extension de corps de $(\mathbb{F}_q)^\theta$ de degré d. Si l'on effectue nd divisions euclidiennes comme précédemment, il existe

une combinaison linéaire non triviale :

$$\sum_{i=0}^{nd} \gamma_i R_i,\ \gamma_i \in (\mathbb{F}_q)^\theta.$$

On conclut comme précédemment que le polynôme $\sum_{i=0}^{dn} \gamma_i X^{is}$ est une borne centrale pour P et que son degré est inférieur ou égal à snd. ∎

Sur $\mathbb{F}_4$, il est possible d'améliorer la borne donnée par le théorème :

Proposition 1.5.5. — *Soit $P \in \mathbb{F}_4[X, \theta]$ où $\theta(x) = x^2$ de degré n, alors il a une borne centrale P^{**} de degré au plus $2n$.*

Remarque 1.5.6. — La majoration du théorème précédent nous donnait $\deg(P^{**}) \leq 4n$.

Démonstration. — Montrons que dans ce cas là il est possible d'exhiber explicitement un polynôme central. Soit :

$$P = \sum_{i=0}^{n} a_i X^i.$$

On va juste montrer que le polynôme $Q = \sum_{j=0}^{n} \theta^{j+1}(a_j) X^j$ convient, c'est-à-dire que l'on va calculer PQ et voir que c'est un polynôme central :

$$PQ = \sum_{i,j,i+j\equiv 1[2]} a_i \theta^{i+j+1}(a_j) X^{i+j} + \sum_{i,j,i+j\equiv 0[2]} a_i \theta^{i+j+1}(a_j) X^{i+j}. \tag{1.9}$$

Etudions chacune des deux sommes de (1.9). Lorsque $i+j$ est impair alors $\theta^{i+j+1}(a_j) = a_j$ et l'on a :

$$\sum_{i,j,i+j\equiv 1[2]} a_i a_j X^{i+j} = 2 \sum_{i<j,i+j\equiv 1[2]} a_i a_j X^{i+j} = 0$$

car on est en caractéristique 2. Pour l'autre somme, on a $\theta^{i+j+1}(a_j) = \theta(a_j)$ et l'on peut écrire :

$$\sum_{i,j,i+j\equiv 0[2]} a_i \theta(a_j) X^{i+j} = \sum_{i,j,i+j\equiv 0[2]} (a_i \theta(a_j) + a_j \theta(a_i)) X^{i+j} + \sum_{i=0}^{n} a_i \theta(a_i) X^{2i}.$$

Chacun des coefficients de cette somme est bien dans $\mathbb{F}_2$ car invariant par θ et les seules puissances de X qui apparaissent dans PQ sont les puissances paires. Le polynôme PQ est bien un polynôme central. En fait, si $PQ = R$, on a :

$$QPQ = QR = RQ = PQQ$$

comme l'anneau est intègre cela montre que $PQ = QP$ et l'on a bien montré que P a un multiple à gauche central de degré plus petit que $2n$. ∎

Exemple 1.5.7. — On se place toujours dans $\mathbb{F}_4[X,\theta]$ et on garde les mêmes notations que dans les exemples précédents. Soit $P = X^7 + \alpha X^6 + \alpha X^5 + \alpha$, on a :

$$P^* = X^{12} + X^{10} + X^8 + \alpha X^6 + \alpha^2 X^4 + X^2 + \alpha^2$$

$$P^{**} = X^{14} + X^{10} + 1.$$

On voit que la borne peut être de degré strictement plus petit que la borne centrale.

1.6 Automorphisme et anti-isomorphisme

Nous allons mettre en évidence une famille d'automorphismes de $\mathbb{F}_q[X,\theta]$ dont nous nous servirons ultérieurement. Puis, nous verrons en nous basant sur la même idée un lien entre $\mathbb{F}_q[X,\theta]$ et $\mathbb{F}_q[X,\theta^{-1}]$.

Soit σ un automorphisme de $\mathbb{F}_q$, on regarde l'application :

$$\begin{array}{rccc} \varphi_\sigma & : & \mathbb{F}_q[X,\theta] & \to & \mathbb{F}_q[X,\theta] \\ & & \sum_{i=0}^{n} a_i X^i & \mapsto & \sum_{i=0}^{n} \sigma(a_i) X^i. \end{array}$$

Proposition 1.6.1. — *Pour tout σ, l'application φ_σ est un automorphisme de $\mathbb{F}_q[X,\theta]$.*

Démonstration. — L'application φ_σ est clairement un morphisme additif. De plus, on a pour tout $a \in \mathbb{F}_q$:

$$\varphi_\sigma(aX) = \sigma(a)X$$

et

$$\varphi_\sigma(a)\varphi_\sigma(X) = \sigma(a)X.$$

Il reste encore à vérifier que :

$$\varphi_\sigma(Xa) = \varphi_\sigma(X)\varphi_\sigma(a).$$

Cela revient à montrer que :

$$\sigma(\theta(a))X = \theta(\sigma(a))X.$$

Ce qui est vrai puisque le groupe des automorphismes d'un corps fini est commutatif. Pour conclure, remarquons que l'inverse de φ_σ est $\varphi_{\sigma^{-1}}$, ce qui montre que φ_σ est bien un automorphisme. ∎

Définition 1.6.2. — *Soit A et B deux anneaux, on dit qu'ils sont **anti-isomorphes** lorsqu'il existe une bijection $\varphi : A \mapsto B$ telle que $\forall (x,y) \in A^2$:*

$$\varphi(0_A) = 0_B,\ \varphi(x+y) = \varphi(x) + \varphi(y)$$

$$\varphi(1_A) = 1_B,\ \varphi(xy) = \varphi(y)\varphi(x).$$

Proposition 1.6.3. — *L'application suivante est un anti-isomorphisme d'anneau :*

$$\begin{array}{rccc} \varphi & : & \mathbb{F}_q[X,\theta] & \to & \mathbb{F}_q[Y,\theta^{-1}] \\ & & \sum_{i=0}^{n} a_i X^i & \mapsto & \sum_{i=0}^{n} \theta^{-1}(a_i) Y^i. \end{array}$$

Démonstration. — Le fait que ce soit un morphisme pour l'addition et une bijection ensembliste est évident. Soit :

$$P = \sum_{i=0}^{m} a_i X^i$$

$$Q = \sum_{j=0}^{n} b_j X^j.$$

On a alors :

$$\varphi(PQ) = \varphi(\sum_{i=0}^{m}\sum_{j=0}^{n} a_i\theta^i(b_j)X^{i+j}) = \sum_{i=0}^{m}\sum_{j=0}^{n} \theta^{-i-j}(a_i)\theta^{-j}(b_j)Y^{i+j}$$

et d'autre part

$$\varphi(Q)\varphi(P) = (\sum_{j=0}^{n} \theta^{-j}(b_j)Y^j)(\sum_{i=0}^{m} \theta^{-i}(a_i)Y^i) = \sum_{i=0}^{m}\sum_{j=0}^{n} \theta^{-j}(b_j)\theta^{-j}(\theta^{-i}(a_i))Y^{i+j}.$$

Ce qui démontre le résultat. ∎

On peut également démontrer que c'est le seul cas où l'on a un anti-isomorphisme.

Théorème 1.6.4. — *Les anneaux $\mathbb{F}_q[X,\theta_1]$ et $\mathbb{F}_q[Y,\theta_2]$ sont anti-isomorphes si et seulement si $\theta_1 = \theta_2^{-1}$.*

Démonstration. — La condition suffisante vient d'être vue. Soit φ un anti-isomorphisme alors, comme dans la démonstration du théorème 1.7, on obtient que φ restreint à $\mathbb{F}_q$ est un automorphisme et $\varphi(X) = aY+b$. Calculons $\varphi(X\alpha)$, où $\alpha \in \mathbb{F}_q$, de deux façons différentes :

$$\varphi(X\alpha) = \varphi(\alpha)\varphi(X) = \varphi(\alpha)(aY+b) = a\varphi(\alpha)Y + b\varphi(\alpha).$$

D'autre part :

$$\varphi(X\alpha) = \varphi(\theta_1(\alpha)X) = \varphi(X)\varphi(\theta_1(\alpha)) = (aY+b)\varphi(\theta_1(\alpha)) = a\theta_2(\varphi(\theta_1(\alpha)))Y + b\varphi(\theta_1(\alpha)).$$

Les automorphismes de $\mathbb{F}_q$ commutent donc :

$$\forall \alpha \in \mathbb{F}_q,\ \theta_2(\theta_1(\alpha)) = \alpha.$$

Ce qui démontre le résultat. ∎

1.7 Factorisation et irréductibilité

1.7.1 Notion de racine

Nous avons vu que nous disposons de beaucoup d'outils dans ce cadre non-commutatif qui sont dérivés du cadre commutatif classique. Une question naturelle qui arrive assez vite est : peut-on parler de racine de ces polynômes ? Cette question est intéressante dans l'optique d'utiliser l'anneau $\mathbb{F}_q[X,\theta]$ pour fabriquer des codes correcteurs puisque, par exemple, les codes BCH utilisent de manière cruciale la notion de racine d'un polynôme générateur.

L'approche naturelle qui consiste à remplacer l'indéterminée X par un élément de $\mathbb{F}_q$ ne marche pas pour la raison simple que le morphisme d'évaluation n'est plus un morphisme dans le cas non-commutatif. Voyons cela sur l'exemple suivant :

Exemple 1.7.1. — On se place dans $\mathbb{F}_4[X,\theta]$ muni de l'automorphisme $\theta(x) = x^2$, on note α le générateur de $\mathbb{F}_4^*$ donné par Magma dans sa version 2.13, nous avons l'égalité suivante :

$$X^2 + 1 = (X + \alpha)(X + \alpha^2).$$

En remplaçant X par 1 nous obtenons alors $0 = 1$. Ce qui montre que l'évaluation ainsi définie n'est pas un morphisme multiplicatif.

En résumé, la valeur du polynôme en un point dépend de la forme sous laquelle on présente ce polynôme. Ce constat fâcheux, nous incite à prendre une autre définition de la notion de racine d'un polynôme :

Définition 1.7.2. — *Soit $f \in \mathbb{F}_q[X,\theta]$ et $s \in \mathbb{N}^*$. On dit que $\alpha \in \mathbb{F}_{q^s}$ est une **racine** de f lorsque $X - \alpha$ divise à droite f dans $\mathbb{F}_{q^s}[X,\theta]$.*

Remarque 1.7.3. — Lorsque $s > 1$, il convient de préciser la signification de $\mathbb{F}_{q^s}[X,\theta]$, en effet un automorphisme θ possède plusieurs extensions à un sur-corps. Ici l'on prendra l'extension qui garde la même expression, c'est-à-dire si $\theta(x) = x^{q_0}$ on prendra pour automorphisme de $\mathbb{F}_{q^s}$:

$$\Theta(x) = x^{q_0}$$

que l'on notera encore, par abus de notation, θ.

Nous allons expliciter un peu cette notion de racine, en la reliant à la notion de racine usuelle d'un polynôme de $\mathbb{F}_q[X]$. Ceci est notamment expliqué dans [13].

Définition 1.7.4. — *Soit θ un automorphisme de $\mathbb{F}_q$ et $\alpha \in \mathbb{F}_{q^s}$, on pose pour tout entier $i \geq 1$:*

$$N_i(\alpha) = \theta^{i-1}(\alpha)\theta^{i-2}(\alpha)...\alpha \tag{1.10}$$

et $N_0(\alpha) = 1$.

Proposition 1.7.5. — *Soit $f = a_nX^n + ... + a_0 \in \mathbb{F}_q[X, \theta]$ et $\alpha \in \mathbb{F}_{q^s}$, le reste de la division euclidienne à droite de f par $X - \alpha$ est :*

$$\sum_{i=0}^{n} a_i N_i(\alpha).$$

Démonstration. — Soit $f(X) = a_nX^n + ... + a_0$ de degré au moins 1. Remarquons l'identité suivante dans $\mathbb{F}_{q^s}[X, \theta]$ valable pour tout entier $i \geq 1$

$$X^i - N_i(\alpha) = [X^{i-1} + \theta^{i-1}(\alpha)X^{i-2} + \theta^{i-1}(\alpha)\theta^{i-2}(\alpha)X^{i-3} + ... + N_i(\alpha)](X - \alpha).$$

En effet, il se produit simplement un télescopage des termes.
En multipliant ces égalités par a_i et en sommant sur i, nous obtenons :

$$\sum_{i=1}^{n} a_iX^i - a_iN_i(\alpha) = Q(X)(X - \alpha).$$

Il reste à ajouter a_0 pour obtenir :

$$f(X) = Q(X)(X - \alpha) + \sum_{i=0}^{n} a_iN_i(\alpha).$$

Ce qui démontre la proposition. ∎

Corollaire 1.7.6. — *Soit $f = a_nX^n + ... + a_0 \in \mathbb{F}_q[X, \theta]$ et $\alpha \in \mathbb{F}_{q^s}$, α est une racine de f si et seulement si :*

$$\sum_{i=0}^{n} a_iN_i(\alpha) = 0.$$

Remarquons ensuite que si $\theta(x) = x^{q_0}$ est distinct de l'identité, alors $N_i(\alpha) = \theta^{i_1}(\alpha)...\alpha = \alpha^{q_0^{i-1}}...\alpha$, c'est-à-dire que :

$$N_i(\alpha) = \alpha^{\sum_{j=0}^{i-1} q_0^j} = \alpha^{\frac{q_0^i - 1}{q_0 - 1}}.$$

On en déduit la proposition suivante :

Proposition 1.7.7. — *Soit $f = a_nX^n + ... + a_0 \in \mathbb{F}_q[X, \theta]$, $\alpha \in \mathbb{F}_{q^s}$ est racine de f si et seulement α est racine du polynôme de $\mathbb{F}_q[Y]$ suivant :*

$$\mathcal{P}_f = \sum_{i=0}^{n} a_iY^{\frac{q_0^i - 1}{q_0 - 1}}. \tag{1.11}$$

Remarque 1.7.8. — Ce polynôme est noté avec l'indéterminée Y en effet c'est pour ne pas le confondre avec nos polynômes tordus, ici c'est bien un polynôme de $\mathbb{F}_q[Y]$ donc commutatif.

Remarque 1.7.9. — La proposition précédente peut paraître suprenante, elle implique qu'un polynôme $f \in \mathbb{F}_q[X,\theta]$ de degré n possède $\frac{q_0^n-1}{q_0-1}$ racines comptées éventuellement avec multiplicité. Voyons l'exemple suivant pour éclaircir cela.

Exemple 1.7.10. — Soit $\theta(x) = x^2$ et le polynôme $f = X^2 + 1 \in \mathbb{F}_4[X,\theta]$. D'après la proposition précédente une racine de f est une racine du polynôme de $\mathbb{F}_4[Y]$ suivant :

$$\mathcal{P}_f = Y^3 + 1.$$

Ce polynôme possède 3 racines que sont 1, α, α^2. Ainsi le polynôme f doit avoir 3 racines, c'est-à-dire 3 facteurs à droite de degré 1 unitaire. Ces racines se trouvent dans $\mathbb{F}_4$ puisque l'on a :

$$X^2 + 1 = (X + 1)(X + 1)$$
$$X^2 + 1 = (X + \alpha)(X + \alpha^2)$$
$$X^2 = (X + \alpha^2)(X + \alpha).$$

Nous aurons l'occasion de retrouver ce fait suprenant dans le chapitre 4, où l'on liera les racines d'un polynôme tordu aux solutions d'une équation aux différences.

1.7.2 Factorisation

En non-commutatif la notion de **polynôme irréductible** est bien définie, c'est également un polynôme non inversible, f, qui n'a pas de factorisation propre sous la forme $f = gh$.

L'anneau $\mathbb{F}_q[X,\theta]$ est euclidien à droite et à gauche, cependant il n'est pas factoriel puisque nous avons vu que l'unicité de la décomposition d'un polynôme en facteurs irréductibles n'est clairement pas au rendez-vous, comme le montre le calcul de l'exemple 1.7.10.

Néanmoins, en suivant le théorème 1.2.9 de [13], nous voyons qu'il existe un équivalent du théorème d'unicité de la décomposition en facteurs irréductibles. Tout d'abord définissons la notion de polynômes semblables.

Notation 4. — Si $a, b \in \mathbb{F}_q[X,\theta]$, on note $(a,b)_d$ le plus grand commun diviseur à droite de a et b, $(a,b)_g$ sera le plus grand commun diviseur à gauche.

Définition 1.7.11. — *Soit f et g deux polynômes non nuls de $\mathbb{F}_q[X,\theta]$, f est dit* ***semblable*** *à gauche au polynôme g s'il existe u et u' dans $\mathbb{F}_q[X,\theta]$ tels que :*

1. $(u', f)_g = 1$.
2. $(u, g)_d = 1$.
3. $u'g = fu$.

Si f est semblable à gauche à g, on note $f \sim_g g$.

Remarque 1.7.12. — Voyons, en commutatif, c'est-à-dire lorsque $\theta = Id$, ce que signifient ces trois conditions. Les conditions 1 et 3 impliquent que $u'|u$, les conditions 2 et 3 impliquent que $u|u'$ donc $u = \lambda u'$ avec λ un scalaire. Etre semblable est synomyme d'être associé pour des polynômes commutatifs.

Exemple 1.7.13. — Dans $\mathbb{F}_4[X,\theta]$, le polynôme $X+1$ est semblable à gauche à $X+\alpha$, en effet :

$$\alpha(X+\alpha) = (X+1)\alpha^2.$$

Nous en arrivons au théorème fondamental suivant qui décrit l'arithmétique de $\mathbb{F}_q[X,\theta]$. Il est énoncé dans [13] de manière très générale pour un anneau principal à gauche et à droite.

Théorème 1.7.14. — *Un élément $P \in \mathbb{F}_q[X,\theta]$, non constant, peut s'écrire sous la forme :*

$$P = P_1 ... P_r \tag{1.12}$$

où les P_i sont irréductibles. De plus si l'on a deux écritures :

$$P = P_1 ... P_r = \hat{P}_1 ... \hat{P}_s$$

alors $r = s$ et il existe $\sigma \in \mathcal{S}_n$ tel que pour tout i, $P_i \sim_g \hat{P}_{\sigma(i)}$.

Exemple 1.7.15. — Dans $\mathbb{F}_4[X,\theta]$, nous avons les factorisations en irréductibles :

$$X^2+1 = (X+1)(X+1)$$

$$X^2+1 = (X+\alpha)(X+\alpha^2).$$

Nous avons vu que $X+1 \sim_g X+\alpha$ mais on a aussi $X+1 \sim_g X+\alpha^2$.

Beaucoup de questions autour de la factorisation des polynômes tordus sont traitées dans [11] où des algorithmes explicites sont donnés et analysés.

Pour la démonstration de ce résultat nous renvoyons à [13] qui utilise le langage des modules et le fait que si l'élément f est irréductible alors l'idéal à gauche engendré par f est maximal.

1.7.3 Polynômes irréductibles

Le nombre de polynômes irréductibles de $\mathbb{F}_q[X,Id]$ est très bien connu, il est donné par la formule suivante où I_t désigne le nombre d'irréductibles unitaires de degré t où $t \geq 2$:

$$I_t = \frac{1}{t}\sum_{d|t} \mu(d) q^{\frac{t}{d}}.$$

La fonction μ étant la fonction de Moebius. On peut trouver une preuve de ce résultat dans la démonstration du théorème 3.25 dans [14].

Cette formule se démontre avec deux ingrédients, le premier est le fait que le polynôme $X^{q^m} - X$ est le produit de tous les polynômes unitaires irréductibles de $\mathbb{F}_q[X]$ dont le degré divise m, puis une utilisation astucieuse de la formule d'inversion de Moebius permet d'obtenir ce résultat. Une étude plus précise de cette formule montre qu'il existe un irréductible de tout degré.

Dans le cadre non-commutatif, la démonstration de cette formule n'est pas possible à appliquer directement, cependant, l'article [6] présente la généralisation de cette formule.

Le langage employé dans cet article est légèrement différent puisque les auteurs parlent de polynômes linéarisés, nous verrons au chapitre 4 l'analogie avec notre cadre.

Théorème 1.7.16. — *Soit $\mathbb{F}_q$ un corps fini de caractéristique p avec $q = p^e$ et $\theta(x) = x^{p^s}$, notons k le pgcd de e et s. Notons $\mathcal{N}_t$ le nombre d'irréductibles unitaires de degré t de $\mathbb{F}_q[X, \theta]$. Alors $\mathcal{N}_1 = q$ et pour tout $t \geq 2$:*

$$\mathcal{N}_t = \frac{q^t - 1}{t(p^{tk} - 1)} \sum_{i|t} \mu(\frac{t}{i})(p^k)^i. \tag{1.13}$$

Remarque 1.7.17. — On retrouve la même formule que dans le cadre commutatif puisqu'alors $s = 0$ et $k = e$.

Remarque 1.7.18. — Ce nombre d'irréductibles ne dépend pas réellement de $\theta = x^{p^s}$ mais juste de e et de s. C'est-à-dire que dans $\mathbb{F}_{16}$,par exemple, donc avec $e = 4$, si l'on considère les automorphismes : $\theta_1(x) = x^{2^1}$, $\theta_2(x) = x^{2^2}$, $\theta_3(x) = x^{2^3}$, alors comme $pgcd(4, 1) = pgcd(4, 3)$, les anneaux $\mathbb{F}_{16}[X, \theta_1]$ et $\mathbb{F}_{16}[X, \theta_3]$ ont le même nombre d'irréductibles d'un degré fixé. Nous avions déjà une première intuition d'un cas particulier de ce résultat avec la proposition 1.6.3 qui disait que $\mathbb{F}_q[X, \theta]$ et $\mathbb{F}_q[X, \theta^{-1}]$ sont anti-isomorphes. Ils ont, en particulier, le même nombre d'irréductibles d'un degré fixé.

Une analyse de cette formule permet de montrer qu'il existe des polynômes irréductibles de $\mathbb{F}_q[X, \theta]$ de tout degré.

Voici quelques résultats sur le nombre d'irréductibles. On remarque qu'il y a toujours moins d'irréductibles en non-commutatif qu'en commutatif.

$\mathbb{F}_4[X, \theta]$:

t	$\theta(x) = x$	$\theta(x) = x^2$
2	6	5
3	20	18
4	60	51
5	204	198
6	670	585
7	2340	2322
8	8160	7710

$\mathbb{F}_{16}[X, \theta]$:

t	$\theta(x) = x$	$\theta(x) = x^2$	$\theta(x) = x^4$	$\theta(x) = x^8$
2	120	85	102	85
3	1360	1170	1300	1170
4	16320	13107	15420	13107

$\mathbb{F}_9[X, \theta]$:

t	$\theta(x) = x$	$\theta(x) = x^3$
2	36	30
3	240	224
4	1620	1476
5	11808	11712

Exemple 1.7.19. — La liste des polynômes irréductibles de degré 2 unitaires de $\mathbb{F}_4[X,\theta]$ est :

$$f_1 = X^2 + \alpha$$
$$f_2 = X^2 + \alpha^2$$
$$f_3 = X^2 + \alpha X + 1$$
$$f_4 = X^2 + \alpha^2 X + 1$$
$$f_5 = X^2 + X + 1.$$

En se souvenant de l'application φ_θ introduite à la proposition 1.6.1 , nous voyons que $f_1 = \varphi_\theta(f_2)$ et $f_3 = \varphi_\theta(f_4)$ et le polynôme f_5 étant à coefficients dans $\mathbb{F}_2$, il satisfait $\varphi_\theta(f_5) = f_5$.

1.8 Polynômes tordus avec dérivation

Nous allons étudier une généralisation de notre anneau $\mathbb{F}_q[X,\theta]$ en introduisant une forme supplémentaire de non-commutativité. C'est sous cette forme-là que Ore dans [21] avait introduit ces anneaux non-commutatifs.

Nous nous servirons de cette généralisation au chapitre 3, lorsque nous étudierons les codes modules.

1.8.1 Définition

Soit $\mathbb{F}_q$ un corps fini, on considère l'ensemble suivant :

$$\mathbb{F}_q[X,\theta,\delta] = \{\sum_{i=0}^{n} a_i X^i,\ a_i \in \mathbb{F}_q,\ n \in \mathbb{N}\}.$$

L'addition est l'addition usuelle sur les polynômes, par contre nous avons la règle de multiplication suivante :

$$\forall a \in \mathbb{F}_q,\ Xa = \theta(a)X + \delta(a). \tag{1.14}$$

On souhaite que la multiplication soit distributive par rapport à l'addition ce qui impose que pour tout a et b dans $\mathbb{F}_q$:

$$X(a+b) = Xa + Xb.$$

Ce qui se traduit par

$$\theta(a+b) = \theta(a) + \theta(b)$$
$$\delta(a+b) = \delta(a) + \delta(b).$$

On aimerait également que $\mathbb{F}_q[X,\theta,\delta]$ soit associatif, c'est-à-dire que :

$$X(ab) = (Xa)b$$

ce qui donne :

$$\theta(ab) = \theta(a)\theta(b)$$
$$\delta(ab) = \theta(a)\delta(b) + \delta(a)b. \tag{1.15}$$

Définition 1.8.1. — *Soit θ un automorphisme de $\mathbb{F}_q$, l'application $\delta : \mathbb{F}_q \mapsto \mathbb{F}_q$ est une* ***θ-dérivation*** *si pour tout a et b dans $\mathbb{F}_q$:*

1. $\delta(a+b) = \delta(a) + \delta(b)$.
2. $\delta(ab) = \theta(a)\delta(b) + \delta(a)b$.

Remarque 1.8.2. — On veut aussi que 1 reste l'élément neutre à droite de $\mathbb{F}_q[X, \theta, \delta]$, c'est-à-dire que $X.1 = X$, ce qui impose :

$$\theta(1) = 1$$

$$\delta(1) = 0.$$

Définition 1.8.3. — *Soit θ un automorphisme de $\mathbb{F}_q$ et δ une θ-dérivation de $\mathbb{F}_q$, on a alors défini un anneau non-commutatif de polynômes : $\mathbb{F}_q[X, \theta, \delta]$.*

En effet en étendant la règle 1.14 par associativité et distributivité, la structure d'anneau est bien définie.

Si l'on connaît parfaitement les automorphismes de $\mathbb{F}_q$, en revanche les θ-dérivations sont moins connues. Nous allons pouvoir dans la suite caractériser les θ-dérivations de $\mathbb{F}_q$.

Nous allons tout d'abord démontrer un lemme qui nous donne $\delta(a^n)$ en fonction de $\delta(a)$ et $\theta(a)$, il nous servira plus tard dans nos démonstrations.

1.8.2 Lemme calculatoire

Lemme 1.8.4. — *Soit $\mathbb{F}_q$ un corps fini, θ un automorphisme de $\mathbb{F}_q$ et δ une θ-dérivation de $\mathbb{F}_q$ alors pour tout $a \in \mathbb{F}_q$ et pour tout $n \geq 1$ on a la relation :*

$$\delta(a^n) = \delta(a)[\sum_{i=0}^{n-1} a^i \theta(a)^{n-1-i}]. \tag{1.16}$$

Démonstration. — On démontre simplement cela par récurrence, pour $n = 1$ le résultat est évident. Pour $n = 2$, il s'agit juste de remarquer que :

$$\delta(a^2) = \delta(a \times a) = \theta(a)\delta(a) + \delta(a)a = \delta(a)[\theta(a) + a]$$

ce qui correspond à la formule annoncée.
On suppose donc la propriété vérifiée au rang n. Ensuite, on remarque que $\delta(a^{n+1}) = \delta(a^n \times a) = \theta(a^n)\delta(a) + \delta(a^n)a$ puisque δ est une θ-dérivation. Il suffit de remplacer $\delta(a^n)$ par son expression provenant de l'hypothèse de récurrence. On obtient donc :

$$\delta(a^{n+1}) = \delta(a)[\theta(a^n) + \sum_{i=0}^{n-1} a^{i+1}\theta(a)^{n-1-i}].$$

Ce qui à un changement d'indice près dans la somme correspond bien au résultat annoncé.

■

Ce résultat est une règle de calcul fondamentale parce que tous les éléments non nuls d'un corps fini peuvent s'écrire comme des puissances d'un élément primitif.

1.8.3 Cas où il n'existe pas de θ-dérivations non triviales

Notons $D_\theta(\mathbb{F}_q)$ l'ensemble des θ-dérivations de $\mathbb{F}_q$. On remarque immédiatement que l'application $\delta = 0$ convient pour être une θ-dérivation. Dans le cas où le corps fini est de cardinal premier, c'est la seule dérivation possible.

Proposition 1.8.5. — *$D_\theta(\mathbb{Z}/p\mathbb{Z})$ est réduit à l'application nulle.*

Démonstration. — Il suffit de remarquer que comme $\delta(1) = 0$ et que δ est un morphisme additif alors :

$$\delta(1 + ... + 1) = 0$$

ce qui assure que δ est identiquement nulle. ∎

Pour avoir des dérivations non triviales, il va falloir se placer sur des extensions de corps plus élaborées, ce qui tombe bien puisque les automorphismes des $\mathbb{Z}/p\mathbb{Z}$ sont triviaux.

Il n'y a également aucune dérivation non nulle lorsque θ est l'identité.

Proposition 1.8.6. — *Soit $q = p^t$ où p est un nombre premier alors $D_{Id}(\mathbb{F}_q)$ est réduit à l'application nulle.*

Démonstration. — On reprend les notations de la proposition et on voit $\mathbb{F}_q$ comme étant $\mathbb{F}_p[X]/\langle f\rangle$ où f est un polynôme irréductible de degré t sur $\mathbb{F}_p[X]$ tel que $\alpha = \bar{X}$ soit un générateur de $(\mathbb{F}_q)^*$. On suppose qu'il existe une dérivation non triviale, c'est-à-dire que $\delta(\alpha) \neq 0$. Comme $\theta = id$, on a d'après le lemme 1.16 :

$$\delta(\alpha^i) = \delta(\alpha)[i\alpha^{i-1}].$$

D'autre part, soit $f(X) = \sum_{i=0}^{r} a_i X^i$ alors $f(\alpha) = 0$ donc $\delta(f(\alpha)) = 0$ et par linéarité de δ on a :

$$\sum_{i=1}^{r} \delta(a_i\alpha^i) = 0.$$

Or les coefficients a_i sont dans $\mathbb{F}_p$ ce qui implique que $\delta(a_i) = 0$ et donc $\delta(a_i\alpha^i) = a_i\delta(\alpha^i)$. On obtient alors :

$$\sum_{i=1}^{r} a_i\delta(\alpha)[ia^{i-1}] = 0$$

$$\sum_{i=1}^{r} a_i[i\alpha^{i-1}] = 0.$$

Il suffit de remarquer que les éléments $1, \alpha, ..., \alpha^{r-1}$ sont libres sur $\mathbb{F}_p$, par construction de $\mathbb{F}_q$. Donc pour tout $i \in \{1...r\}$, on a :

$$a_i i = 0.$$

Cette dernière relation signifie que les seuls coefficients éventuellement non nuls de f sont ceux associés aux puissances de la caractéristique, p. Dans une telle situation, un résultat classique nous dit que f est la puissance p-ième d'un polynôme, en particulier n'est pas irréductible. Ce qui est absurde. ∎

1.8.4 Etude générale des θ-dérivations de $\mathbb{F}_q$

Voyons tout d'abord un exemple pour se convaincre que de tels objets existent.

Exemple 1.8.7. — On se place dans $\mathbb{F}_4$ et on note α un générateur de $\mathbb{F}_4^*$. On prend $\theta(x) = x^2$. On pose :

$$\delta(0) = \delta(1) = 0$$

$$\delta(\alpha) = \delta(\alpha^2) = \alpha.$$

Il est évident et rapide de vérifier la linéarité de δ ainsi que la propriété de θ-dérivation.

On obtient un nouvel anneau non-commutatif de polynômes $\mathbb{F}_q[X, \theta, \delta]$ dans lequel nous avons par exemple :

$$(X + 1)(X + \alpha) = X^2 + \alpha X.$$

Voyons ce qui se passe en toute généralité. Soit $\mathbb{F}_q$ un corps fini où $q = p^t$. Prenons un automorphisme de ce corps fini : $\theta(x) = x^{p^r}$. Le but est de déterminer toutes les θ-dérivations de $\mathbb{F}_q$. Notons comme précédemment $\mathbb{F}_q = \mathbb{F}_p/\langle f \rangle$ où f est un polynôme irréductible de degré t tel que $\alpha = \overline{X}$ soit un élément primitif de $\mathbb{F}_q$. Supposons qu'il existe une θ-dérivation non nulle et notons-là δ. D'après 1.16, donner $\delta(\alpha)$ suffit à déterminer parfaitement la θ-dérivation.

En posant $\delta(\alpha) = \beta$ avec $\beta \neq 0$, on obtient la formule suivante :

$$\delta(\alpha^i) = \beta[\alpha^{i-1} + \alpha^{i-2}\theta(\alpha) ... + \theta(\alpha)^{i-1}], \tag{1.17}$$

avec $\delta(0) = \delta(1) = 0$. Toutes les θ-dérivations non nulles sont donc de cette forme, il s'agit de montrer que la formule ci-dessus est bien une θ-dérivation.

Proposition 1.8.8. — *Ainsi définie δ est une θ-dérivation.*

Démonstration. — Il va falloir vérifier la propriété de θ-dérivation et la linéarité de δ pour montrer ce résultat.
Montrons que pour tous indices i et j, on a bien :

$$\delta(\alpha^{i+j}) = \theta(\alpha^i)\delta(\alpha^j) + \delta(\alpha^i)\alpha^j.$$

C'est immédiat à vérifier, en effet on a :

$$\delta(\alpha^{i+j}) = \beta[\alpha^{i+j-1} + \alpha^{i+j-2}\theta(\alpha) ... + \theta(\alpha)^{i+j-1}]$$

et d'autre part :

$$\theta(\alpha^i)\delta(\alpha^j) + \delta(\alpha^i)\alpha^j = \theta(\alpha)^i\beta[\alpha^{j-1} + ... + \theta(\alpha)^{j-1}] + \beta\alpha^j[\alpha^{i-1} + ... + \theta(\alpha)^{i-1}]$$

$$= \beta[\alpha^{i+j-1} + ... + \alpha^j\theta(\alpha)^{i-1} + \alpha^{j-1}\theta(\alpha)^i + ... + \theta(\alpha)^{i+j-1}].$$

Ce qui correspond bien.

Vérifions à présent la linéarité. La relation fondamentale qui donne le lien entre tous les α^i est $f(\alpha) = 0$, c'est-à-dire $\sum_{i=0}^{t} a_i \alpha^i = 0$.

Il suffit de vérifier que $\sum_{i=0}^{t} a_i \delta(\alpha^i) = 0$. L'application nulle étant évidemment une dérivation, on suppose que $\beta \neq 0$.
On a :

$$\begin{aligned}\sum_{i=0}^{t} a_i \delta(\alpha^i) &= \beta \sum_{i=1}^{s} a_i [\alpha^{i-1} + ... + \theta(\alpha)^{i-1}] \\ &= \beta \sum_{i=1}^{s} a_i [\alpha^{i-1} + \alpha^{i-2+p^r} + ... + \alpha^{(i-1)p^r}] \\ &= \beta \sum_{i=1}^{s} a_i [\alpha^{i-1} \frac{1 - \alpha^{(p^r-1)i}}{1 - \alpha^{p^r-1}}] \\ &= \frac{\beta}{1 - \alpha^{p^r-1}} \sum_{i=1}^{s} a_i [\alpha^{i-1} - \alpha^{p^r i-1}].\end{aligned}$$

Regardons en premier lieu la somme :

$$\sum_{i=1}^{s} a_i \alpha^{i-1} = \frac{1}{\alpha}(f - a_0)(\alpha) = -\frac{a_0}{\alpha}.$$

Montrons qu'elle est égale à l'autre somme :

$$\sum_{i=1}^{s} a_i \alpha^{p^r i-1} = \frac{1}{\alpha}(f - a_0)(\alpha^{p^r}) = \frac{1}{\alpha}[f(\alpha^{p^r}) - a_0] = -\frac{a_0}{\alpha}$$

puisque $f(\alpha^{p^r}) = f(\alpha)^{p^r} = 0$.
On a bien :

$$\sum_{i=0}^{s} a_i \delta(\alpha^i) = 0.$$

Il est également évident de vérifier que si $\alpha^{i_0} \in \mathbb{F}_p$ alors on a $\delta(\alpha^{i_0}) = 0$, en effet :

$$\delta(\alpha^{i_0}) = \beta \alpha^{i_0-1} \frac{1 - \alpha^{(p^r-1)i_0}}{1 - \alpha^{p^r-1}}.$$

Or $\alpha^{i_0(p^r-1)} = 1$ puisque $\alpha^{i_0 p} = \alpha^{i_0}$.

■

En résumé, on obtient le résultat suivant :

Théorème 1.8.9. — *Soit $\mathbb{F}_q$ muni d'un automorphisme :*

1. *Si $\theta = id$, il n'y a qu'une dérivation, la dérivation triviale.*
2. *Si $\theta \neq id$, il y a q dérivations distinctes données par l'image par la dérivation d'un générateur de $(\mathbb{F}_q)^*$.*

1.8.5 Principales dérivations utilisées

Voici les descriptions des principales dérivations qui vont être utilisées par la suite, notamment au chapitre 3.

On se place dans $\mathbb{F}_4$ muni de l'automorphisme $\theta(x) = x^2$, et l'on note α un générateur de $\mathbb{F}_4^*$, voici les θ-dérivations non nulles de $\mathbb{F}_4$:

	δ_1	δ_2	δ_3
0	0	0	0
1	0	0	0
α	1	α	α^2
α^2	1	α	α^2

Nous utiliserons également, au chapitre 4, la θ-dérivation suivante définie sur $\mathbb{F}_8$ muni de $\theta(x) = x^2$, on note toujours α le générateur de $\mathbb{F}_8^*$ donné par Magma dans sa version 2.13. On choisit $\delta(\alpha) = \alpha$:

$$\delta(0) = \delta(1) = 0$$

$$\delta(\alpha) = \delta(\alpha^3) = \alpha$$

$$\delta(\alpha^2) = \delta(\alpha^6) = \alpha^5$$

$$\delta(\alpha^4) = \delta(\alpha^5) = \alpha^6.$$

Enfin donnons un dernier exemple de θ-dérivation de $\mathbb{F}_{16}$ muni de $\theta(x) = x^4$. Notons α le générateur donné par Magma, il vérifie d'ailleurs $\alpha^4 + \alpha + 1 = 0$, on choisit $\delta(\alpha) = \alpha^6$:

$$\delta(\alpha) = \alpha^6,\ \delta(\alpha^2) = \alpha^6,\ \delta(\alpha^3) = \alpha$$

$$\delta(\alpha^4) = \alpha^6,\ \delta(\alpha^5) = 0,\ \delta(\alpha^6) = \alpha^{11}$$

$$\delta(\alpha^7) = \alpha^{11},\ \delta(\alpha^8) = \alpha^6,\ \delta(\alpha^9) = \alpha^{11}$$

$$\delta(\alpha^{10}) = 0,\ \delta(\alpha^{11}) = \alpha,\ \delta(\alpha^{12}) = \alpha$$

$$\delta(\alpha^{13}) = \alpha^{11},\ \delta(\alpha^{14}) = \alpha, \delta(\alpha^{15}) = 0.$$

1.8.6 Propriétés de $\mathbb{F}_q[X, \theta, \delta]$

Nous avons comme dans le cas où il n'y a pas de dérivation :

Proposition 1.8.10. — *Soit P et Q appartenant à $\mathbb{F}_q[X, \theta, \delta]$, non nuls.*
(i) $\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\}$.
(ii) $\deg(PQ) = \deg(P) + \deg(Q)$.

Démonstration. — L'assertion (ii) se vérifie en remarquant que si $f = a_n X^n + ... + a_0$ et $g = b_m X^m + ... + b_0$ alors

$$fg = a_n \theta^n(b_m) X^{n+m} + ...$$

■

Remarque 1.8.11. — Les termes de degré plus petit que $n + m$ sont beaucoup plus complexes à écrire puisqu'ils sont sommes de plusieurs termes. Il nous faudrait connaître une expression de $X^n a$ sous forme d'un polynôme. Nous ferons cela très précisément au chapitre 4 afin d'avoir l'expression des coefficients de la matrice génératrice d'un code correcteur.

On en déduit que $\mathbb{F}_q[X, \theta, \delta]$ est un anneau intègre.

Il est également très intéressant de remarquer qu'il existe encore une division euclidienne à droite ou à gauche dans cet anneau-là. En effet nous pouvons faire s'annuler le terme de tête d'un polynôme quelconque f avec un multiple d'un polynôme non nul g. Plus précisément, nous avons par exemple la division euclidienne à droite :

Théorème 1.8.12. — *Soient f et g dans $\mathbb{F}_q[X, \theta]$ avec $g \neq 0$, il existe q et r dans $\mathbb{F}_q[X, \theta, \delta]$ tels que :*

$$f = qg + r$$

et

$$\deg(r) < \deg(g).$$

Cette propriété va nous permettre de travailler facilement avec des idéaux et de manipuler également des codes correcteurs construits à l'aide de polynômes de $\mathbb{F}_q[X, \theta, \delta]$.

Le seul bémol est que les idéaux bilatères de $\mathbb{F}_q[X, \theta, \delta]$ sont beaucoup moins simples à caractériser que ceux de $\mathbb{F}_q[X, \theta]$, c'est pour cela que nous ne reverrons l'anneau $\mathbb{F}_q[X, \theta, \delta]$ qu'au chapitre 4 où l'on va s'affranchir des idéaux bilatères.

Chapitre 2

Construction de θ-codes

L'introduction de l'anneau de polynômes tordus vue au chapitre précédent va à présent nous permettre de fabriquer des codes correcteurs. Cette construction fut mise au point en 2007 par Ulmer, Boucher et Geiselmann dans l'article [31] qui ont dans un premier temps étudié uniquement les codes cycliques, c'est-à-dire engendrés par un polynôme dont la borne est de la forme $X^n - 1$. Puis ce travail a été généralisé dans [30] avec notamment l'étude de la dualité euclidienne et hermitienne de ces codes.

Nous rappellerons la construction classique des codes θ-cycliques. Puis, par analogie avec ce cadre commutatif, nous définirons les θ-codes dans la définition 2.2.2. Nous obtiendrons également une matrice génératrice de ces codes. On verra quelques exemples et un tableau de résultats afin de connaître les paramètres des codes ainsi créés et la distance minimale de ces codes nous intéressera plus particulièrement. Enfin en suivant [30] nous donnerons les principaux résultats concernant la dualité ; nous verrons en particulier que le dual d'un code θ-cyclique est un code θ-cyclique au théorème 2.5.4. Une caractérisation, un algorithme et une méthode de détermination des codes seront également donnés.

2.1 Codes cycliques usuels

Nous allons commencer par rappeler brièvement la méthode de construction des codes cycliques. Il sera intéressant de garder en tête ce processus étant donné que l'extension au cadre non-commutatif se fera avec la même idée. On considère l'application décalage circulaire suivante :

$$\begin{array}{rccc} \tau & : & \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ & & (a_0, a_1, ..., a_{n-1}) & \mapsto & (a_{n-1}, a_0, ..., a_{n-2}). \end{array}$$

Définition 2.1.1. — *Soit $\mathcal{C}$ un code linéaire sur $\mathbb{F}_q$, on dit que $\mathcal{C}$ est* ***cyclique*** *lorsque :*

$$x \in \mathcal{C} \iff \tau(x) \in C. \tag{2.1}$$

Exemple 2.1.2. — Plaçons-nous sur $\mathbb{F}_2$ et prenons le code de longueur 7 engendré par :

$$m_0 = (1,1,0,1,0,0,0)$$
$$m_1 = (0,1,1,0,1,0,0)$$
$$m_2 = (0,0,1,1,0,1,0)$$
$$m_3 = (0,0,0,1,1,0,1).$$

On peut vérifier que ces 4 vecteurs forment une base d'un code de dimension 4 qui est cyclique. En effet :

$$m_1 = \tau(m_0)$$
$$m_2 = \tau(m_1)$$
$$m_3 = \tau(m_2)$$
$$\tau(m_3) = m_0 + m_1 + m_2.$$

L'introduction de cette nouvelle condition va nous permettre d'utiliser l'outil polynomial pour manipuler les codes correcteurs. On considère l'application :

$$\begin{array}{rccc} T & : & \mathbb{F}_q^n & \to & \mathbb{F}[X]/\langle X^n-1\rangle \\ & & (a_0,a_1,...,a_{n-1}) & \mapsto & a_0+a_1X+...+a_{n-1}X^{n-1}. \end{array}$$

On a le lien fondamental suivant :

Proposition 2.1.3. — *Soit $\mathcal{C}$ un code linéaire sur $\mathbb{F}_q$, alors $\mathcal{C}$ est **cyclique** si et seulement si $T(\mathcal{C})$ est un **idéal** de $\mathbb{F}_q[X]/\langle X^n-1\rangle$.*

Démonstration. — La preuve est classique et consiste à faire le calcul suivant dans l'anneau quotient $\mathbb{F}_q[X]/\langle X^n-1\rangle$.

$X(a_0+a_1X+...+a_{n-1}X^{n-1}) = a_0X+a_1X^2...+a_{n-1}X^n = a_{n-1}+a_0X+...+a_{n-2}X^{n-1}$.

Ce qui établit clairement que pour $x \in \mathcal{C}$, $T(\tau(x)) = XT(x)$. Le décalage circulaire correspond donc bien à la stabilité par multiplication par X via l'application T. ∎

Des résultats de la théorie des anneaux nous disent que les idéaux de $\mathbb{F}_q[X]/\langle X^n-1\rangle$ sont principaux et sont en bijection avec les diviseurs unitaires de X^n-1. Plus précisément, on a le résultat suivant :

Théorème 2.1.4. — *Soient :*

$$g(X) = a_0 + ... + X^r$$

un diviseur unitaire de X^n-1 dans $\mathbb{F}_q[X]$ et :

$$m = (a_0,...,1,0,...,0)$$

le mot correspondant. Alors les $n-r$ mots de codes :

$$m = (a_0, ..., 1, 0, ..., 0)$$
$$\tau(m) = (0, a_0, ..., 1, 0, ..., 0)$$
$$...$$
$$\tau^{n-r-1}(m) = (0, ..., 0, a_0, ..., 1)$$

forment une base d'un code cyclique de dimension $n-r$. Réciproquement tout code cyclique de longueur n sur $\mathbb{F}_q$ s'obtient par la construction précédente.

Les codes cycliques sont une famille de codes correcteurs extrêmement utilisée dans les applications. On sait construire de tels codes en prescrivant la distance minimale, ce sont les codes BCH. L'avantage de ces codes est notamment que l'on dispose d'un algorithme de décodage rapide et utilisant principalement l'algorithme d'Euclide polynomial, cette façon de décoder sera d'ailleurs transposable aux codes que l'on va étudier au paragraphe 3.3.5 du chapitre 3.

2.2 Définition des θ-codes

Nous allons calquer la construction précédente, l'anneau $\mathbb{F}_q[X]$ va être remplacé par $\mathbb{F}_q[X, \theta]$.

Soit I un idéal bilatère de $\mathbb{F}_q[X, \theta]$, alors I est principal et est généré à droite (et à gauche aussi d'après le lemme 1.4.4) par un polynôme f. Le quotient $\mathbb{F}_q[X, \theta]/\langle f\rangle$ a une structure naturelle d'anneau. C'est un $\mathbb{F}_q$-espace vectoriel dont une base est $\{1, ..., X^{\deg(f)-1}\}$. On a le résultat suivant qui généralise la situation du cas commutatif.

Proposition 2.2.1. — *Les idéaux à gauche de $\mathbb{F}_q[X, \theta]/\langle f\rangle$ sont principaux et engendrés par la classe d'un diviseur à droite de f dans $\mathbb{F}_q[X, \theta]$.*

Démonstration. — Soit J un idéal à gauche non réduit à zéro de $\mathbb{F}_q[X, \theta]/\langle f\rangle$. Choisissons un polynôme unitaire de J de plus petit degré et notons le G. Soit $P \in J$, si l'on effectue la division euclidienne à droite de P par G dans $\mathbb{F}_q[X, \theta]$ (en voyant P et G comme des éléments de $\mathbb{F}_q[X, \theta]$), on a :

$$P = QG + R$$

où $\deg(R) < \deg(G) < \deg(f)$. Donc $R = P - QG$ (ou plutôt sa classe dans $\mathbb{F}_q[X, \theta]$) est dans J, c'est absurde sauf si $R = 0$. On a alors $J = \langle G\rangle_g$. De plus G est un diviseur à droite de f car la classe de f, qui est 0, est bien dans l'idéal engendré par G. ∎

On peut maintenant donner la définition d'un θ-code.

Définition 2.2.2. — *Soit $\mathcal{C}$ un code linéaire de longueur n sur $\mathbb{F}_q$. C'est un* ***θ-code*** *s'il existe $f \in \mathbb{F}_q[X, \theta]$ tel que $\langle f\rangle$ soit un idéal bilatère et*

$$J = \{a_0 + a_1X + ... + a_{n-1}X^{n-1},\ (a_0, a_1, ..., a_{n-1}) \in \mathcal{C}\}$$

soit un idéal à gauche de $\mathbb{F}_q[X, \theta]/\langle f\rangle$. D'après la proposition précédente les éléments de J sont des multiples à gauche d'un diviseur à droite, g, de f.

Notation 5. — On notera parfois $\langle g\rangle/\langle f\rangle$ le code défini ci-dessus.

Cette définition est la généralisation naturelle du cas commutatif qui correspond à $\theta = Id$. La famille de codes obtenue est plus vaste mais partage de nombreuses propriétés avec les codes cycliques commutatifs. On va pouvoir, comme dans le cas commutatif utiliser des techniques sur les polynômes afin de travailler sur les codes. Nous prescrirons notamment la distance minimale d'un code au chapitre 3 en généralisant les codes BCH classiques.

Définition 2.2.3. — *Si de plus f est dans le centre de $\mathbb{F}_q[X,\theta]$, on dit que $\mathcal{C}$ est un* ***θ-code central****.*

Définition 2.2.4. — *Si $f = X^n - 1$ où $|<\theta>|$ divise n (afin que f génère bien un idéal bilatère) alors $\mathcal{C}$ est appelé code* ***θ-cyclique****.*

Il est possible de donner la matrice génératrice d'un θ-code. Si $g = g_0 + g_1X + ... + g_rX^r$ divise $f \in \mathbb{F}_q[X,\theta]$ tel que $\langle f\rangle)$ soit un idéal bilatère, alors :

$$\{m(X)g(X),\ \deg(m(X)) \leq n-r-1\}$$

forme l'ensemble des mots du code vu ici de manière polynomiale. En remarquant que :

$$X^i g(X) = \sum_{j=0}^{r} \theta^i(g_j)X^{i+j}$$

il est possible de former une matrice génératrice du code :

$$\begin{pmatrix} g_0 & \cdots & g_{r-1} & g_r & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \cdots & \theta(g_{r-1}) & \theta(g_r) & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \theta^{n-r-1}(g_0) & \cdots & \theta^{n-r-1}(g_{r-1}) & \theta^{n-r-1}(g_r) \end{pmatrix}.$$

Il s'agit d'une matrice à $n-r$ lignes et n colonnes. De manière similaire aux codes cycliques, la propriété d'être un idéal se répercute sur les mots du code.

2.3 Propriétés sur les mots de code et exemples

Voyons tout d'abord ce qui se passe dans le cas θ-cyclique ainsi qu'un exemple.

Proposition 2.3.1. — *Soit $\mathcal{C}$ un code linéaire sur $\mathbb{F}_q$ alors $\mathcal{C}$ est un code θ-cyclique si et seulement si :*

$$(a_0, ..., a_1, ..., a_{n-1}) \in \mathcal{C} \Longleftrightarrow (\theta(a_{n-1}), \theta(a_0), ..., \theta(a_{n-2})) \in \mathcal{C}.$$

Démonstration. — Il s'agit simplement de montrer, comme dans le cas commutatif, que la condition :

$$(a_0, ..., a_1, ..., a_{n-1}) \in \mathcal{C} \Longleftrightarrow (\theta(a_{n-1}), \theta(a_0), ..., \theta(a_{n-2})) \in \mathcal{C}$$

est équivalente à la stabilité par multiplication par X. Si $u = (a_0, a_1, ..., a_{n-1})$, notons $u^\theta = (\theta(a_{n-1}), \theta(a_0), ..., \theta(a_{n-2}))$. Soit $u \in \mathcal{C}$ et P_u le polynôme de $\mathbb{F}_q[X, \theta]/\langle X^n - 1\rangle$ qui lui est canoniquement associé, alors :

$$XP_u(X) = X(\sum_{i=0}^{n-1} a_i X^i) = \sum_{i=0}^{n-1} \theta(a_i) X^{i+1} = P_{u^\theta}(X).$$

Ce qui démontre l'équivalence annoncée puisque la stabilité par multiplication par X et la linéarité suffisent pour avoir un idéal dans ce cas. ∎

Voyons tout de suite un premier exemple explicite.

Exemple 2.3.2. — On se place dans $\mathbb{F}_4[X, \theta]$, où $\theta(x) = x^2$ et on note $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$. On considère le polynôme :

$$f = X^8 - 1$$

qui génère bien un idéal bilatère puisque f est central d'après le théorème 1.4.6. On a la factorisation suivante :

$$X^8 - 1 = (X^3 + \alpha X + \alpha)(X^5 + \alpha^2 X^3 + \alpha^2 X^2 + \alpha X + \alpha^2).$$

Le polynôme $g = X^5 + \alpha^2 X^3 + \alpha^2 X^2 + \alpha X + \alpha^2$ est un diviseur à droite de f, il génère un code θ-cyclique dont la matrice génératrice est :

$$\begin{pmatrix} \alpha^2 & \alpha & \alpha^2 & \alpha^2 & 0 & 1 & 0 & 0 \\ 0 & \alpha & \alpha^2 & \alpha & \alpha & 0 & 1 & 0 \\ 0 & 0 & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & 0 & 1 \end{pmatrix}.$$

Cette matrice est la matrice génératrice d'un code sur $\mathbb{F}_4$ de paramètres $[8, 3, 5]$.

Donnons un exemple où le θ-code que l'on obtient n'est pas θ-cyclique, et voyons la condition qui en découle sur les mots du code.

Exemple 2.3.3. — On se place dans le même cadre, c'est-à-dire que l'on travaille avec l'anneau de polynômes tordus $\mathbb{F}_4[X, \theta]$. On prend pour polynôme central :

$$f = X^{12} + X^6 + X^4 + X^2 + 1$$

et l'on remarque que l'on dispose de la factorisation suivante :

$$f = (X^6 + \alpha X^5 + \alpha^2 X^4 + \alpha^2 X^3 + X^2 + \alpha^2)(X^6 + \alpha X^5 + \alpha X^4 + \alpha^2 X^3 + X^2 + \alpha).$$

Le polynôme $X^6 + \alpha X^5 + \alpha X^4 + \alpha^2 X^3 + X^2 + \alpha$ génère un θ-code qui en plus est central. La matrice génératrice est :

$$\begin{pmatrix} \alpha & 0 & 1 & \alpha^2 & \alpha & \alpha & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^2 & 0 & 1 & \alpha & \alpha^2 & \alpha^2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 1 & \alpha^2 & \alpha & \alpha & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^2 & 0 & 1 & \alpha & \alpha^2 & \alpha^2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha & 0 & 1 & \alpha^2 & \alpha & \alpha & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha^2 & 0 & 1 & \alpha & \alpha^2 & \alpha^2 & 1 \end{pmatrix}.$$

Cela nous donne un code sur $\mathbb{F}_4$ de paramètres $[12, 6, 5]$. Il est en outre possible de trouver une condition sur les mots similaire à celle que l'on trouve dans le cas des codes cycliques ou θ-cycliques. Pour cela il suffit de traduire la condition de stabilité par multiplication par X.

Soit $(a_0, ..., a_{11}) \in \mathcal{C}$ et $P = a_0 + ...a_{11}X^{11}$ son polynôme associé alors $XP(X)$ est un polynôme associé à un mot du code, plus précisément :

$$XP(X) = \theta(a_0)X + ... + \theta(a_{11})X^{12} = \theta(a_0)X + ... + \theta(a_{11})(X^6 + X^4 + X^2 + 1).$$

Il en découle la condition suivante sur les mots de code :

$$(a_0, a_1, ..., a_{11}) \in \mathcal{C}$$

$$\Longleftrightarrow$$

$$(\theta(a_{11}), \theta(a_0), \theta(a_1) + \theta(a_{11}), \theta(a_2), \theta(a_3) + \theta(a_{11}), \theta(a_4), \theta(a_5) + \theta(a_{11}), ..., \theta(a_{10})) \in \mathcal{C}.$$

La condition de stabilité par multiplication par X peut toujours être traduite par une condition sur les mots du code plus ou moins compliquée.

2.4 Etude quantitative des θ-codes

Nous allons voir dans ce paragraphe un tableau donnant les meilleures distances minimales obtenues à l'aide de θ-codes et nous allons les comparer aux meilleures distances minimales connues. Cela nous permettra de voir que l'ensemble des θ-codes contient de bons codes. Mais voyons tout d'abord que cette famille de codes est strictement plus grande que la famille des codes cycliques, ce qui n'était a priori pas tout à fait clair. Les résultats suivants ainsi que le tableau sont issus de [30].

Proposition 2.4.1. — *Soit $f = X^n - 1$ un polynôme de $\mathbb{F}_q[X, \theta]$ qui génère un idéal bilatère. Un code θ-cyclique engendré par un diviseur à droite unitaire, g, de f de degré inférieur ou égal à $n - 1$ est cyclique si et seulement si tous les coefficients de g sont dans $\mathbb{F}_q^\theta$.*

Démonstration. — Soit $g = X^r + \sum_{i=0}^{r-1} g_i X^i$. Tout d'abord si tous les coefficients de g sont dans $(\mathbb{F}_q)^\theta$ alors la matrice génératrice est la matrice d'un code cyclique. Réciproquement si le θ-code généré par g est cyclique, alors $gX \in \mathcal{C}$. Comme le code est linéaire, on a en particulier $Xg - gX \in \mathcal{C}$. C'est-à-dire :

$$(\theta(g_0) - g_0)X + (\theta(g_1) - g_1)X^2 + ... + (\theta(g_{r_1}) - g_{r_1})X^r$$

est un multiple à gauche de g, notons le λg. Comme g divise f son terme constant n'est pas nul. Donc nécessairement $\lambda = 0$ et donc le polynôme $Xg - gX$ est nul. Les g_i sont invariants par θ d'où le résultat. ∎

L'étude de la famille des θ-codes est liée au nombre de facteurs à droite d'un polynôme central, voyons quelques résultats sur la factorisation d'un polynôme central. Tout d'abord un exemple.

Exemple 2.4.2. — On se place dans $\mathbb{F}_4[X,\theta]$, où θ est l'automorphisme de Frobenius et on note α un générateur de $\mathbb{F}_4^*$. On a les factorisations suivantes :

$$\begin{aligned} X^4+X^2+1 &= (X^2+X+1)(X^2+X+1) \\ &= (X^2+\alpha^2)(X^2+\alpha) \\ &= (X^2+\alpha)(X^2+\alpha^2) \\ &= (X^2+\alpha^2X+1)(X^2+\alpha X+1) \\ &= (X^2+\alpha X+1)(X^2+\alpha^2X+1). \end{aligned}$$

En regardant ces factorisations, on aboutit au lemme suivant, en notant $Z(\mathbb{F}_q[X,\theta])$ le centre de l'anneau $\mathbb{F}_q[X,\theta]$.

Lemme 2.4.3. — *Si $h.g \in Z(\mathbb{F}_q[X,\theta])$, alors h et g commutent.*

Démonstration. — Comme $h.g$ est dans le centre de $\mathbb{F}_q[X,\theta]$, on a $(h.g).h = h.(h.g)$, et comme on travaille dans un anneau intègre cela donne en simplifiant par h, $h.g = g.h$. ∎

D'autre part si l'on reprend les notations du chapitre précédent, c'est-à-dire si l'on pose :

$$\begin{array}{rccc} \varphi_\sigma & : & \mathbb{F}_q[X,\theta] & \to & \mathbb{F}_q[X,\theta] \\ & & \displaystyle\sum_{i=0}^{n} a_iX^i & \mapsto & \displaystyle\sum_{i=0}^{n} \sigma(a_i)X^i \end{array}$$

on a alors le résultat suivant :

Lemme 2.4.4. — *Soit f un polynôme central qui a pour factorisation $f = g.h$ alors pour tout $i \in \mathbb{N}$, on a :*

$$f = \varphi_{\theta^i}(g)\varphi_{\theta^i}(h).$$

Démonstration. — Il suffit de se souvenir que φ_{θ^i} est un morphisme d'anneau et que f est à coefficients dans le corps fixe de θ. ∎

Les deux lemmes précédents permettent d'éclairer un peu la factorisation donnée dans l'exemple. Il est intéressant de se demander si les codes obtenus possèdent de bons paramètres. En théorie des codes, le paramètre que l'on veut en général optimiser à longueur et dimension fixée est la distance minimale. Dans le tableau de résultats suivant on travaille dans $\mathbb{F}_4$. En ligne la longueur n du code, en colonne le degré r du polynôme générateur, c'est-à-dire que la dimension du code est $n-r$. Pour n et r fixés ce tableau donne la distance minimale et la nature du code obtenu. Plus précisément, C_d signifie qu'il existe un code cyclique de distance minimale d, C_d^θ veut dire qu'il existe un code θ-cyclique et non cyclique de distance minimale d, le symbole θ_d signifie qu'il existe un code θ-central mais pas de code θ-cyclique, enfin si jamais à n et r fixés, on ne trouve pas de code θ-cyclique

atteignant la meilleure distance minimale connue on indique la différence entre ces deux distances minimales par un nombre négatif. Ce tableau est exhaustif.

n/r	2	3	4	5	6	7	8	9	10
4	C_3^θ	C_4							
6	C_2	C_4	C_4^θ	C_6					
8	C_2	C_3^θ	C_4^θ	C_5^θ	C_6^θ	C_8			
10	C_2	θ_3	C_4^θ	C_5^θ	C_6^θ	θ_6	θ_8	C_{10}	
12	C_2	θ_3	θ_4	C_4	C_6^θ	C_6^θ	C_7^θ	C_8^θ	C_9^θ
14	C_2	C_3^θ	C_4^θ	C_4	C_5^θ	C_6^θ	C_7^θ	-1	-1
16	C_2	-1	-1	C_4^θ	-1	-1	-1	-1	C_8^θ
18	C_2	-1	θ_3	θ_4	-1	-1	C_6^θ	-1	C_8^θ
20	-1	θ_3	θ_3	θ_4	-1	-1	θ_6	C_7^θ	C_8^θ
22	θ_2	θ_2	θ_3	θ_4	θ_4	θ_5	-1	C_6^θ	C_7^θ
24	C_2^θ	C_2^θ	θ_3	C_4^θ	C_4^θ	-1	-1	C_6^θ	C_7^θ
26	θ_2	θ_2	θ_3	θ_4	θ_4	-1	-1	C_6^θ	C_7^θ
28	C_2^θ	C_2^θ	θ_3	C_4^θ	C_4^θ	-1	θ_5	C_6^θ	C_6^θ
30	C_2^θ	C_2^θ	C_3^θ	C_4^θ	C_4^θ	-1	C_5^θ	C_6^θ	C_6^θ
32	C_2^θ	C_2^θ	-1	-1	θ_4	-1	θ_5	C_6^θ	θ_6
34	θ_2	θ_2	-1	-1	θ_4	-1	C_5^θ	C_6^θ	C_6^θ
36	C_2^θ	C_2^θ	-1	-1	θ_4	-1	-1	-1	θ_6
38	θ_2	θ_2	-1	-1	θ_4	-1	-1	-1	θ_6
40	C_2^θ	C_2^θ	-1	-1	θ_4	-1	-1	-1	θ_6
42	C_2^θ	C_2^θ	-1	C_3^θ	C_4^θ	-1	-1	-1	C_6^θ
44	C_2^θ	C_2^θ	-1	θ_3	θ_4	θ_4	-1	-1	-1

Au delà du degré 10, il n'est plus possible de continuer de manière exhaustive ce tableau pour des raisons de temps de calcul. Ce tableau montre que notre famille de θ-codes atteint assez souvent la meilleure distance minimale possible. De plus, nous voyons que les codes θ-cycliques sont souvent strictement meilleurs que les codes cycliques que l'on pourrait obtenir avec un même jeu de paramètres.

Hormis la distance minimale, il peut être intéressant d'optimiser le polynôme énumérateur de poids du code.

Définition 2.4.5. — *Soit $\mathcal{C}$ un code sur $\mathbb{F}_q$, on note de manière usuelle $\omega(c)$ le poids d'un mot $c \in \mathcal{C}$ et on appelle* ***polynôme énumérateur de poids*** *de $\mathcal{C}$, le polynôme :*

$$P_{\mathcal{C}} = \sum_{c \in \mathcal{C}} Y^{\omega(c)}.$$

Le rôle de ce polynôme est clair : si la distance minimale est un paramètre primordial du code, il est évidemment intéressant de se demander combien de mots atteignent ce poids.

Définition 2.4.6. — *On dit que le code $\mathcal{C}$ a une meilleure répartition de poids que le code $\mathcal{C}'$ s'il existe $p \in \mathbb{N}^*$ tel que :*

$$(P_{\mathcal{C}} - P_{\mathcal{C}'})^{(p)}(0) < 0,\ (P_{\mathcal{C}} - P_{\mathcal{C}'})^{(i)}(0) = 0,\ \forall i \in \{0, ..., p-1\}.$$

Dans beaucoup de cas, on se rend compte que les θ-codes que l'on obtient ont une meilleure répartition de poids que les meilleurs codes donnés par le logiciel Magma dans sa version 2.13.

Exemple 2.4.7. — Le meilleur code de paramètres $[6, 2, 4]$ sur $\mathbb{F}_4$ donné par Magma a pour polynôme énumérateur de poids $1 + 15Y^4$. Tandis que le θ-code sur $\mathbb{F}_4$ muni de l'automorphisme de Frobenius généré par $X^4 + X^3 + \alpha^2X^2 + X + \alpha$ qui a pour borne $X^6 + X^4 + X^2 + 1$ a pour polynôme énumérateur de poids :

$$P = 1 + 3Y^4 + 12Y^5.$$

Il a un meilleur polynôme énumérateur de poids.

Il faut cependant pondérer cela, car l'implémentation des meilleurs codes dans Magma n'a sûrement pas été faite pour optimiser cette répartition de poids.

2.5 Dualité

On peut munir $\mathbb{F}_q^n$ du produit scalaire suivant :

Définition 2.5.1. — *Soit $x = (x_1, ..., x_n) \in \mathbb{F}_q^n$ et $y = (y_1, ..., y_n) \in \mathbb{F}_q^n$, on définit le* ***produit scalaire euclidien*** *de x et y par :*

$$< x, y >= \sum_{i=1}^{n} x_i y_i. \tag{2.2}$$

Définition 2.5.2. — *Soit $\mathcal{C}$ un code, on appelle dual euclidien de $\mathcal{C}$, le code défini par :*

$$\mathcal{C}^{\perp} = \{x \in \mathbb{F}_q^n,\ \forall y \in \mathcal{C},\ < x, y >= 0\}.$$

On dit qu'un code est auto-dual lorsque $\mathcal{C} = \mathcal{C}^{\perp}$.

Ces notions ont un intérêt important dans plusieurs questions intéressantes autour des codes. Plus précisément, l'objet jouant un rôle primordial est l'enveloppe d'un code $\mathcal{C}$ définie par $\mathcal{H}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^{\perp}$. La connaissance de la dimension de l'enveloppe permet de contrôler la complexité d'algorithmes de séparation du support qui interviennent dans des questions d'équivalence de codes. Pour plus de détails, on pourra se référer à [26] et [27]. L'algorithme de séparation du support intervient également dans le cryptosystème de McEliece et dans le calcul du groupe d'automorphismes d'un code.

L'article [30] montre que le dual d'un code θ-cyclique est un code θ-cyclique ; nous allons ici expliquer cette preuve. Tout d'abord pour aboutir à ce résultat, nous allons devoir étudier la matrice de parité d'un code θ-cyclique :

Lemme 2.5.3. — *On se place dans $\mathbb{F}_q$ muni d'un automorphisme θ. On suppose que l'ordre de θ divise n afin que $X^n - 1$ soit un polynôme central. Soit $X^n - 1 = hg$ et on note $\mathcal{C}$ le code θ-cyclique engendré par g. Si $h = h_0 + h_1X + ...h_{n-r}X^{n-r}$, alors la matrice suivante est une matrice de parité du code $\mathcal{C}$:*

$$H = \begin{pmatrix} h_{n-r} & \cdots & \theta^{n-r-1}(h_1) & \theta^{n-r}(h_0) & 0 & \cdots & 0 \\ 0 & \theta(h_{n-r}) & \cdots & \cdots & \theta^{n-r+1}(h_0) & \cdots & 0 \\ 0 & \ddots & \ddots & & & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 & \\ 0 & \cdots & 0 & \theta^{r-1}(h_{n-r}) & \cdots & \theta^{n-2}(h_1) & \theta^{n-1}(h_0) \end{pmatrix}.$$

Ce résultat est démontré dans [30].

Grâce à ce résultat, nous sommes en mesure de déduire le théorème suivant :

Théorème 2.5.4. — *On se place dans $\mathbb{F}_q$ muni de l'automorphisme θ et l'on suppose que l'ordre de θ divise n. Soit $g = g_0 + ... + g_r X^r$ et $h = h_0 + ... + h_{n-r}X^{n-r}$ des élements de $\mathbb{F}_q[X,\theta]$ tels que $hg = X^n - 1$. Le dual du code θ-cyclique engendré par g dans $\mathbb{F}_q[X,\theta]/\langle X^n - 1\rangle$ est le code θ-cyclique engendré par :*

$$g^\perp = h_{n-r} + \theta(h_{n-r-1})X + ... + \theta^{n-r}(h_0)X^{n-r}.$$

La matrice de parité H du code est la matrice génératrice du code dual et l'on voit que cette matrice de parité est bien la matrice d'un code θ-cyclique sous réserve que $g^\perp$ divise bien $X^n - 1$. Ce fait est démontré dans [30] en utilisant l'objet $\mathbb{F}_q(X,\theta)$ qui est le corps à droite des fractions de $\mathbb{F}_q[X,\theta]$.

Exemple 2.5.5. — On se place dans $\mathbb{F}_4[X,\theta]$ avec l'automorphisme $\theta(x) = x^2$ et on note α un générateur de $(\mathbb{F}_4)^*$. Soit $g = X^2 + \alpha X + \alpha^2$ et $h = X^2 + \alpha X + \alpha$, nous avons $X^4 - 1 = gh$ et le polynôme $g^\perp = \alpha X^2 + \alpha^2 X + 1 = \alpha g$. Donc le code θ-cyclique engendré par g est auto-dual. C'est un code de paramètres $[4, 2, 2]$.

Ce beau résultat pour les codes θ-cycliques ne se généralise pas au cas des codes θ-centraux puisque le dual d'un code θ-central n'est pas forcément un code θ-central.

Les codes auto-duaux jouant un rôle particulier, nous avons envie d'utiliser le théorème précédent afin de disposer d'un moyen de les trouver. Il suffit en fait d'écrire que le polynôme $g^\perp$ est proportionnel à g afin qu'ils engendrent le même code. Plus précisément, en gardant les notations du théorème précédent, nous devons avoir $g^\perp = \theta^r(h_0)g$. En identifiant les coefficients, nous obtenons des équations polynomiales sur les coefficients g_i. Il est possible d'utiliser des bases de Gröbner pour trouver tous les polynômes g qui conviennent. Cette solution est mise en oeuvre dans [30]. Nous obtenons une liste de codes θ-cycliques qui sont auto-duaux, certains atteignent les meilleures distances minimales connues pour des codes auto-duaux.

Nous pouvons également définir une autre notion de dualité dans notre cadre :

Définition 2.5.6. — *On prend q une puissance paire d'un nombre premier et $\theta(x) = x^{\sqrt{q}}$. Soient $x = (x_1, ..., x_n) \in \mathbb{F}_q^n$ et $y = (y_1, ..., y_n) \in \mathbb{F}_q^n$, on définit le* ***produit scalaire hermitien*** *de x et y par :*

$$< x, y >_H = \sum_{i=1}^{n} x_i\theta(y_i). \tag{2.3}$$

On note $\mathcal{C}^H$ le dual hermitien d'un code $\mathcal{C}$.

Nous avons alors un théorème similaire au précédent qui nous dit, sous des conditions de dimension du code toutefois plus restrictives, que le dual hermitien d'un code θ-cyclique est un code θ-cyclique.

Théorème 2.5.7. — *En gardant les mêmes hypothèses que dans la définition précédente, soit g et $h = h_0 + ... + h_r X^r$ des éléments de $\mathbb{F}_q[X, \theta]$ tels que $X^{2r} - 1 = hg$. Le dual hermitien du code θ-cyclique engendré par g dans $\mathbb{F}_q[X, \theta]/\langle X^{2r} - 1\rangle$ est un code θ-cyclique engendré par :*

$$g^H = \theta^{m-1}(h_r) + \theta^m(h_{r-1})X + ... + \theta^{m+r-1}(h_0)X^r.$$

La démonstration de ce résultat est présentée dans [30]. Il est également possible, en tout cas pour des corps assez petits, de donner exhaustivement la liste des codes θ-cycliques auto-duaux pour la dualité hermitienne, à l'aide des bases de Gröbner. Les tableaux de résultats sont présentés dans l'article [30].

Chapitre 3

Prescription de la distance minimale

Nous allons voir dans ce chapitre une méthode de construction de θ-codes qui va nous permettre de minorer la distance minimale. Nous verrons deux approches pour faire cela, la première méthode de construction permettra de minorer la distance rang du code. Les codes que l'on obtiendra par ce biais ont déjà été en partie étudiés par Gabidulin dans [9], cependant notre méthode sera plus générale. La seconde approche généralisera les codes BCH. Cette famille de codes étudiée par exemple au chapitre 6 de [32] permet de construire des codes ayant une distance minimale minorée. Cette construction est généralisable pour notre anneau $\mathbb{F}_q[X, \theta]$. Ces deux méthodes nous permettront d'obtenir des codes correcteurs ayant une meilleure distance minimale que ceux connus jusqu'à présent d'après le site **http ://www.codetables.de/** qui les recense. En particulier nous obtiendrons un code de paramètres $[42, 14, 21]$ sur $\mathbb{F}_8$ dans l'exemple 3.2.14 et un code de paramètres $[40, 23, 10]$ sur $\mathbb{F}_4$ dans l'exemple 3.3.8 qui améliorent tous deux de 1 la meilleure distance minimale connue jusqu'alors.

Tout d'abord, nous parlerons de la théorie des équations aux différences qui va être l'outil fondamental de ce chapitre ; cette théorie a été abondamment étudiée notamment dans [28] dans un cadre très général, le fait de travailler ici sur un corps fini va nous permettre de simplifier beaucoup cette théorie et d'obtenir des solutions sans passer par le corps de Picard-Vessiot. Nous verrons que les équations aux différences sont exactement le même objet que les polynômes linéarisés qui sont introduits et étudiés dans [14]. Le lien fondamental entre équations aux différences et polynômes tordus sera mis en lumière dans la proposition 3.1.15. Puis nous passerons, dans le paragraphe 2, à un algorithme de construction explicite de code dont le rang est prescrit. Nous donnerons plusieurs exemples et des tableaux de résultats. Nous construirons dans le paragraphe 3 des codes BCH non-commutatifs et nous donnerons pour finir un algorithme de décodage de ces codes.

Ce chapitre est adapté de l'article co-écrit avec Felix Ulmer et Pierre Loidreau : "Skew codes of prescribed distance or rank".

3.1 Théorie des opérateurs aux différences

Dans ce paragraphe nous allons étudier la notion d'opérateurs aux différences et nous allons

voir le lien fort entre ces opérateurs et l'anneau non-commutatif $\mathbb{F}_q[X, \theta]$.

3.1.1 Définition et premières propriétés

Soit $q = p^r$ où p est un nombre premier et $\theta(x) = x^{p^i}$ avec $i \in \{0...r-1\}$ un automorphisme de $\mathbb{F}_q$.

Définition 3.1.1. — *Une* ***équation aux différences*** *sur* $(\mathbb{F}_q, \theta)$ *est une équation de la forme :*

$$L(y) = a_n\theta^n(y) + ... + a_1\theta(y) + a_0 y = 0 \tag{3.1}$$

où les a_i *sont des éléments de* $\mathbb{F}_q$*.*

Il est possible de chercher des solutions à cette équation dans $\mathbb{F}_q$, bien sûr, mais également dans une extension de corps en étendant l'automorphisme θ, plus précisément nous avons :

Définition 3.1.2. — *On dit que le corps aux différences* $(\mathbb{F}_{q'}, \Theta)$ *est une extension du corps aux différences de* $(\mathbb{F}_q, \theta)$ *lorsque* $\mathbb{F}_q \subset \mathbb{F}_{q'}$ *et* Θ *est l'automorphisme de* $\mathbb{F}_{q'}$ *défini par* $\Theta(x) = x^{p^i}$*.*

Remarque 3.1.3. — Il y a plusieurs façons d'étendre un automorphisme à une extension de corps. L'exemple le plus simple et le plus révélateur est de prendre $\mathbb{F}_2$ muni de l'automorphisme identité, $\mathbb{F}_4$ est une extension de $\mathbb{F}_2$ et l'identité sur $\mathbb{F}_4$ est bien entendu un prolongement de l'identité sur $\mathbb{F}_2$. Cependant, l'application $\theta(x) = x^2$ définie sur $\mathbb{F}_4$ ne bouge pas les éléments de $\mathbb{F}_2$, c'est également un prolongement de l'identité.

La définition précédente précise que, parmi les prolongements possibles, nous choisirons celui qui garde la même expression formelle.

Il est dès lors possible de chercher des solutions de l'équation aux différences 3.1 dans une extension de corps aux différences. Nous avons le résultat suivant :

Proposition 3.1.4. — *Les solutions de l'équation aux différences* $L(y) = 0$ *sur n'importe quel corps aux différences* $(\mathbb{F}_{q'}, \theta)$ *forment un* $(\mathbb{F}_{q'})^\theta$*-espace vectoriel.*

Démonstration. — Il suffit de remarquer que l'automorphisme θ défini sur $\mathbb{F}_q$ est $(\mathbb{F}_q)^\theta$-linéaire, en effet si $\alpha \in (\mathbb{F}_q^\theta)$ et $(a, b) \in (\mathbb{F}_q)^2$, nous avons :

$$\theta(\alpha a + b) = \theta(\alpha)\theta(a) + \theta(b) = \alpha\theta(a) + \theta(b).$$

Ainsi l'opérateur L qui est combinaison linéaire de puissances de θ est $(\mathbb{F}_q)^\theta$-linéaire, d'où le résultat. ∎

Ce cadre là est très similaire à la théorie de Galois classique des équations aux différences développée dans [28]. Cependant l'existence d'un anneau aux différences de décomposition (anneau de Picard-Vessiot) ne découle pas ici des théorèmes généraux. En effet l'hypothèse fondamentale est le fait que le corps des constantes soit algébriquement clos, les corps finis n'étant pas algébriquement clos ; nous ne sommes pas dans ce cadre là. Néanmoins, nous

allons pouvoir obtenir un résultat similaire étant donné que nous connaissons entièrement la structure et les interactions entre un corps fini et ses extensions.

La première étape consiste à remarquer que l'opérateur L peut s'écrire en fait sous forme de polynôme.

Définition 3.1.5. — *Nous pouvons associer à l'opérateur* $L(y) = a_n\theta^n(y) + ... + a_1\theta(y) + a_0y = 0$ *le polynôme :*

$$\hat{L}(Y) = a_nY^{p^{in}} + ... + a_1Y^{p^i} + a_0Y. \tag{3.2}$$

Ces deux objets sont évidemment les mêmes, juste écrits différemment en se souvenant que $\theta(y) = y^{p^i}$.

Remarque 3.1.6. — Un tel polynôme est appelé p^i-polynôme ou lorsque le contexte est clair un polynôme linéarisé. Ces polynômes qui ont la particularité que l'ensemble de leurs racines ait une structure d'espace vectoriel ont été largement étudiés dans [14] et [20].

Ce lien va nous permettre d'étudier l'ensemble des solutions de l'équation $L(y) = 0$.

Lemme 3.1.7. — *Il existe une extension de* $\mathbb{F}_q$ *qui contient toutes les solutions de* $L(y) = 0$.

Démonstration. — Il suffit de rappeler que le polynôme $\hat{L}$ a un corps de décomposition, c'est-à-dire une extension de $\mathbb{F}_q$ qui contient toutes ses racines. ∎

Nous allons nous intéresser à la dimension de l'espace des solutions de $L(y) = 0$.

En général, le corps fixé par θ dépend du corps dans lequel on considère l'équation. Afin de le fixer nous allons adopter les notations suivantes : $\theta(x) = x^{q_0}$, $q = q_0^t$ et L un opérateur aux différences à coefficients dans $\mathbb{F}_q$. Ainsi quelque soit l'extension de corps dans laquelle on étudiera les solutions de $L(y) = 0$, on aura $(\mathbb{F}_{q^s})^\theta = \mathbb{F}_{q_0}$.

Définition 3.1.8. — *On appelle* ***multiplicité*** *d'une solution* β *de* $L(y) = 0$*, l'ordre de* β *en tant que racine de* $\hat{L}$.

Exemple 3.1.9. — L'opérateur $L(y) = \theta^n(y)$ a pour unique solution 0 qui est de multiplicité q_0^n.

Définition 3.1.10. — *Soit* $L(y) = a_n\theta^n(y)+...+a_1\theta(y)+a_0y$ *un opérateur aux différences, on appelle* ***valuation*** *de* L*, l'entier* $val(L) = \min\{i,\ a_i \neq 0\}$.

Le lemme suivant est une reformulation du théorème 3.50 de [14], nous gardons les notations et conventions introduites précédemment.

Lemme 3.1.11. — *L'ensemble des solutions de* $L(y) = 0$ *est un espace vectoriel sur* $\mathbb{F}_{q_0}$ *et chaque solution a pour multiplicité* $(q_0)^{val(L)}$.

Démonstration. — Tout d'abord remarquons que la dérivée de $\hat{L}$ vaut a_0 donc si $a_0 \neq 0$ toutes les solutions de $L(y) = 0$ ont pour multiplicité 1.
Soit $k = val(L)$, c'est-à-dire $a_0 = a_1 = ... = a_{k-1} = 0$ et $a_k \neq 0$ alors :

$$\hat{L}(Y) = \sum_{i=k}^{n} a_i Y^{q_0^i} = \sum_{i=k}^{n} a_i^{q_0^{tk}} Y^{q_0^i}.$$

La dernière égalité étant vraie puisque a_i appartient à $\mathbb{F}_{q_0^t} = \mathbb{F}_q$. En utilisant le fait que la caractéristique de $\mathbb{F}_q$ divise q_0 nous avons :

$$\hat{L}(Y) = \sum_{i=k}^{n} [a_i^{q_0^{(t-1)k}} Y^{q_0^{i-k}}]^{q_0^k}.$$

Le polynôme entre crochets a son terme constant non nul donc toutes ses racines sont d'ordre 1, donc toutes les solutions de $L(y) = 0$ sont d'ordre q_0^k. ∎

Le théorème suivant résume ce que nous venons d'apprendre :

Théorème 3.1.12. — *Soit θ un automorphisme de $\mathbb{F}_q$ défini par $a \mapsto a^{q_0}$, on pose $q = q_0^t$ et on suppose que $(\mathbb{F}_q)^\theta = \mathbb{F}_{q_0}$. Soit $L(y) = a_n\theta^n(y) + ... + a_1\theta(y) + a_0 y$ avec $a_i \in \mathbb{F}_q$. Il existe un corps fini $\mathbb{F}_{q^s}$ qui contient toutes les solutions de $L(y) = 0$. Cet ensemble de solutions est un espace vectoriel sur $(\mathbb{F}_q)^\theta$ de dimension $n - val(L)$.*

Démonstration. — On note encore $k = val(L)$. Le polynôme $\hat{L}$ est de degré q_0^n, et toutes ses racines sont de multiplicité q_0^k, il possède donc q_0^{n-k} racines. Nous avons vu que ces racines ont une structure d'espace vectoriel sur $\mathbb{F}_{q_0}$, cet espace vectoriel est de dimension $n - k$.

∎

Prenons quelques exemples pour illustrer ce théorème.

Exemple 3.1.13. —

- L'espace des solutions de l'équation aux différences $L(y) = \theta^n(y) - y$ est $\mathbb{F}_{q_0^n}$. C'est bien un espace vectoriel de dimension n sur $\mathbb{F}_{q_0}$, puisque qu'ici $a_0 = -1 \neq 0$.
- L'espace des solutions de $L(y) = \theta^n(y)$ est $\{0\}$. C'est bien un espace vectoriel de dimension 0, en effet ici $a_0 = ... = a_{n-1} = 0$ donc on a bien $val(L) = n$.
- L'espace des solutions de $L(y) = \theta^n(y) - \theta^{n-1}(y)$ est $\mathbb{F}_{q_0}$. Pour voir cela, il suffit de voir que $L(\beta) = 0$ équivaut à $\theta(\beta) - \beta = 0$ donc $\beta \in \mathbb{F}_{q_0}$. Dans ce cas la multiplicité de chaque solution est q_0^{n-1}.

3.1.2 Lien avec les polynômes non-commutatifs

Ce lien a été mis en évidence par Ore dans [20].
Partant de l'équation aux différences $L(y)$ on peut lui associer l'opérateur aux différences :

$$L = a_n\theta^n + ... + a_1\theta + a_0. \tag{3.3}$$

On note $\mathcal{L}(\mathbb{F}_q)$ l'ensemble de ces opérateurs aux différences.

Définition 3.1.14. — *L'ensemble $\mathcal{L}(\mathbb{F}_q)$ peut être muni d'une structure d'anneau $(\mathcal{L}(\mathbb{F}_q), +, \circ)$ où la multiplication $\circ$ est la composition des opérateurs définie par $(L_1 \circ L_2)(y) = L_1(L_2(y))$.*

Nous allons voir le lien entre cet anneau et l'anneau $\mathbb{F}_q[X, \theta]$.

Proposition 3.1.15. — *L'application suivante est un morphisme d'anneau :*

$$\begin{array}{rccc} \psi : & \mathbb{F}_q[X,\theta] & \to & (\mathcal{L}(\mathbb{F}_q), +, \circ) \\ & \sum_{i=0}^{n} a_i X^i & \mapsto & \sum_{i=0}^{n} a_i \theta^i. \end{array}$$

Cette application est une bijection.

Démonstration. — La stabilité par somme est claire, de plus $\psi(aX) = \psi(a) \circ \psi(X)$ mais comme les anneaux sont non-commutatifs, nous devons également vérifier que $\psi(Xa) = \psi(a)\psi(X)$:

$$\psi(Xa) = \psi(\theta(a)X) = \theta(a)\theta$$

et d'autre part :

$$\psi(Xa)(y) = [\psi(X) \circ \psi(a)](y) = \theta(ay) = \theta(a)\theta(y).$$

Donc $\psi(Xa) = \theta(a)\theta$ également. ∎

On va pouvoir se servir de ce lien en théorie des codes puisque l'on sait fabriquer des codes à partir de polynômes tordus.

Un des buts de la suite de ce chapitre va être de construire l'équivalent des codes BCH dans le contexte non-commutatif. La difficulté est que la notion de racine n'est pas clairement définie pour les polynômes tordus. On rappelle la définition de racine d'un polynôme tordu vue au chapitre 1.

Définition 3.1.16. — *Soit $f \in \mathbb{F}_q[X]$, $\alpha \in \mathbb{F}_{q^s}$ est une racine de f si et seulement si f est divisible à droite par $X - \alpha$ dans $\mathbb{F}_{q^s}[X]$.*

La proposition fondamentale suivante montre le lien entre les solutions d'une équation aux différences et une racine d'un polynôme tordu.

Proposition 3.1.17. — *Soit θ un automorphisme de $\mathbb{F}_q$, $L(y) = \sum_{i=0}^{n} a_i \theta^i(y)$ une équation aux différences et $P = \sum_{i=0}^{n} a_i X^i$ le polynôme de $\mathbb{F}_q[X, \theta]$ associé. Un élément non nul, β de $\mathbb{F}_{q^s}$ est une solution de $L(y) = 0$ si et seulement si $X - \frac{\theta(\beta)}{\beta}$ est un diviseur à droite de P dans $\mathbb{F}_{q^s}[X, \theta]$.*

Démonstration. — Supposons que $L(\beta) = 0$. Effectuons la division euclidienne à droite de P par $X - \frac{\theta(\beta)}{\beta}$, nous obtenons :

$$P = Q(X - \frac{\theta(\beta)}{\beta}) + R.$$

Le reste R est une constante, éventuellement nulle. Nous pouvons appliquer ψ^{-1}, voir proposition 3.1.15, afin de voir cette relation dans le monde des opérateurs aux différences. En notant L_S, l'opérateur aux différences associé à un polynôme S, nous avons :

$$L = L_Q(\theta - \frac{\theta(\beta)}{\beta}) + L_R.$$

On remarque que $(\theta - \frac{\theta(\beta)}{\beta})(\beta) = 0$ donc $L_R(\beta) = 0$. Comme R est une constante et que β est non nulle, on en déduit que R est nul.
Réciproquement si $R = 0$ alors $L(\beta) = 0$. ∎

Nous nous servirons de cette correspondance entre solution de $L(y) = 0$ et racine du polynôme tordu associé dans la suite.

3.1.3 Casoratien

Avant de commencer à fabriquer des codes correcteurs à distance prescrite, nous avons besoin d'un dernier outil. Nous allons par la suite prescrire des puissances consécutives d'éléments comme racines d'un polynôme tordu, c'est-à-dire prescrire des solutions à un opérateur aux différences. Pour faire cela, nous avons besoin de pouvoir construire un opérateur aux différences qui a certaines solutions fixées. C'est à cette question que l'on va répondre dans ce paragraphe.

On garde les mêmes notations que précédemment, à savoir $\theta(x) = x^{q_0}$ et $q = q_0^t$.

Définition 3.1.18. — *Soit $\{\beta_1, ..., \beta_n\}$ des éléments de $\mathbb{F}_q$, on appelle* ***Casoratien*** *de $\{\beta_1, ..., \beta_n\}$, le déterminant suivant :*

$$Cas(y_1, ..., y_n, y) = \begin{vmatrix} y_1 & y_2 & \cdots & y_n & y \\ \theta(y_1) & \theta(y_2) & \cdots & \theta(y_n) & \theta(y) \\ \theta^2(y_1) & \theta^2(y_2) & \cdots & \theta^2(y_n) & \theta^2(y) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \theta^n(y_1) & \theta^n(y_2) & \cdots & \theta^n(y_n) & \theta^n(y) \end{vmatrix} = 0.$$

Notons $Cas_i(y_1, ..., y_n)$ le déterminant obtenu à partir du précédent en enlevant la i-ème ligne et la dernière colonne, nous obtenons :

$$Cas(y_1, ..., y_n) = \sum_{i=0}^{n} (-1)^{n+i+2} Cas_{i+1}(y_1, ...y_n)\theta^i(y).$$

Il est agréable de rendre unitaire cet opérateur aux différences, dans la suite nous noterons :

$$L_{y_1,...,y_n} = \theta^n(y) + \sum_{i=0}^{n} (-1)^{n+i+2} \frac{Cas_{i+1}(y_1, ...y_n)}{Cas_{n+1}(y_1, ..., y_n)} \theta^i(y). \tag{3.4}$$

Remarque 3.1.19. — On peut voir le Casoratien comme l'équivalent du Wronskien de la théorie de Galois différentielle.

Proposition 3.1.20. — *Soit $y_1, ..., y_n$ des éléments de $\mathbb{F}_q$ linéairement indépendants sur $\mathbb{F}_{q_0}$. Alors l'ensemble des solutions de l'équation aux différences $Cas(y_1, ..., y_n, y) = 0$ est l'espace vectoriel sur $\mathbb{F}_{q_0}$ engendré par $y_1, ..., y_n$.*

Démonstration. — En développant par rapport à la dernière colonne le Casoratien, nous voyons que c'est un opérateur aux différences classique qui s'écrit sous la forme : $\sum_{i=0}^{n} \alpha_i \theta^i(y)$ où les α_i, qui s'expriment en fonction des $\theta^k(y_j)$, sont des éléments de $\mathbb{F}_q$. En évaluant en y_i cet opérateur aux différences, le déterminant a deux colonnes identiques, donc :

$$\forall i \in \{1...n\},\ Cas(y_1, ..., y_n, y_i) = 0.$$

avec $\gamma_i \in \mathbb{F}_{q_0}$.
L'opérateur aux différences étant $\mathbb{F}_{q_0}$-linéaire, nous avons déjà q_0^n solutions : $Vect_{\mathbb{F}_{q_0}}(\{y_1, ..., y_n\})$. Le polynôme linéarisé correspondant est de degré q_0^n, nous avons donc trouvé toutes les solutions. ∎

Remarque 3.1.21. — Supposons que l'hypothèse d'indépendance linéaire ne soit pas vérifiée, c'est-à-dire :

$$\sum_{i=1}^{n} \gamma_i y_i = 0.$$

Alors en appliquant θ^j à l'équation précédente, nous obtenons :

$$\theta^j(\sum_{i=1}^{n} \gamma_i y_i) = \sum_{i=1}^{n} \gamma_i \theta^j(y_i) = 0$$

étant donné que $\theta(\gamma_i) = \gamma_i$. Cela montre que dans ce cas les n premières colonnes de la matrice du Casoratien sont liées et que l'équation aux différences associée est identiquement nulle.

Même si les éléments $y_1, ..., y_n$ vivent dans une extension de corps assez grande de la forme $\mathbb{F}_{q^s}$, il est tout à fait possible que leur Casoratien soit à coefficients dans un plus petit corps. La proposition précise à quelles conditions ce phénomène se produit.

Lemme 3.1.22. — *Soit $\theta(x) = x^{q_0}$, $q = q_0^t$ et σ un générateur du groupe de Galois de l'extension $\mathbb{F}_{q^s}/\mathbb{F}_q$. Soit $y_1, ..., y_n$ des éléments de $\mathbb{F}_{q^s}$ linéairement indépendants sur $\mathbb{F}_{q_0}$. L'équation aux différences $L_{y_1,...y_n}(y)$ est à coefficients dans $\mathbb{F}_q$ si et seulement si $Vect_{\mathbb{F}_{q_0}}(\{y_1, ...y_n\})$ est stable par σ.*

Démonstration. — Supposons que $L_{y_1,...y_n}(y) = \sum_{i=0}^{n} \alpha_i \theta^i(y)$ avec $\alpha_i \in \mathbb{F}_q$. Comme σ et l'extension de θ à $\mathbb{F}_{q^s}$ commutent, nous avons :

$$0 = \sigma(\sum_{i=0}^{n} \alpha_i \theta^i(y)) = \sum_{i=0}^{n} \alpha_i \theta^i(\sigma(y)).$$

Ce qui montre que l'espace vectoriel sur $\mathbb{F}_{q_0}$ engendré par $y_1, ..., y_n$ est stable par σ. Réciproquement en reprenant l'expression de l'équation 3.4, nous avons le coefficient de $\theta^i(y)$ qui est, au signe près, $\frac{Cas_{i+1}(y_1,...y_n)}{Cas_{n+1}(y_1,...,y_n)}$. Il s'agit de montrer qu'il est invariant sous σ, en effet :

$$\sigma\left(\frac{Cas_{i+1}(y_1,...y_n)}{Cas_{n+1}(y_1,...,y_n)}\right) = \frac{det(\sigma).Cas_{i+1}(y_1,...y_n)}{det(\sigma).Cas_{n+1}(y_1,...,y_n)} = \frac{Cas_{i+1}(y_1,...y_n)}{Cas_{n+1}(y_1,...,y_n)}.$$

■

3.2 Codes tordus avec prescription de la distance rang

3.2.1 La métrique rang

Nous allons dans ce paragraphe définir une autre notion de poids d'un mot et de distance d'un code. Cette notion de **métrique rang** est particulièrement bien adaptée à certains cadres comme la correction d'erreurs "entrelacées" (crisscross error correction), voir par exemple [25].

Si $f \in \mathbb{F}_q[X, \theta]$ génère un idéal bilatère et que $f = hg$, alors tout mot de code c qui appartient au θ-code engendré par la projection dans le quotient $\mathbb{F}_q[X, \theta]/\langle f\rangle$ de l'idéal à gauche $\langle g\rangle$ est représenté de façon unique par un polynôme de $\mathbb{F}_q[X, \theta]$ de degré $n-1$ au plus (n étant le degré de f). C'est-à-dire qu'un mot de code est représenté par un vecteur de longueur n à coefficients dans $\mathbb{F}_q$. Posons $c = (c_1, ..., c_n)$. D'autre part $\mathbb{F}_q$ est un espace vectoriel sur $(\mathbb{F}_q)^\theta$, notons $e_1, ..., e_m$ une base avec $m = [\mathbb{F}_q : (\mathbb{F}_q)^\theta]$. Chaque c_i peut s'écrire dans cette base sous la forme :

$$c_i = \sum_{j=1}^{m} x_{i,j} e_j.$$

On note M_c la matrice $(x_{i,j})_{1\leq i\leq n, 1\leq j\leq m}$ à coefficients dans $(\mathbb{F}_q)^\theta$.

Définition 3.2.1. — *On appelle* ***rang*** *du mot c et on note $Rg(c)$ le rang de la matrice M_c.*

Remarque 3.2.2. — Ce rang est clairement indépendant de la base de $\mathbb{F}_q$ sur $(\mathbb{F}_q)^\theta$ choisie, par contre il dépend évidemment de l'automorphisme θ par conséquent quand nous parlerons de rang d'un mot de code le contexte sera précisé.

Exemple 3.2.3. — Soit $c = (0, 0, \gamma, 0, \beta)$ où $\gamma \in \mathbb{F}_q^*$ et $\beta \in \mathbb{F}_q^*$. Le poids de Hamming de c est égal à 2. Le rang de c vaut 1 ou 2 selon que γ et β soient liés ou non sur $(\mathbb{F}_q)^\theta$.

L'exemple précédent met en évidence la proposition suivante :

Proposition 3.2.4. — *Soit $c \in \mathbb{F}_q^n$, nous avons :*

$$Rg(c) \leq d(c).$$

Démonstration. — Il suffit de remarquer que le rang de c est au plus égal au nombre de composantes non nulles de c. ∎

Définition 3.2.5. — *La **distance rang minimale** d'un code $\mathcal{C}$ est l'entier d défini par :*

$$d = \min_{c \in \mathcal{C} \setminus \{0\}} Rg(c).$$

D'après la proposition précédente la distance rang minimale d'un code est majorée par la distance minimale de Hamming. Cette distance rang a été introduite par Gabidulin dans [9]. Il a étudié des codes qui avait une distance rang optimale une fois la longueur et la dimension du code fixées. Un algorithme de décodage des codes de Gabidulin a été mis en oeuvre dans [15]. Enfin une application à la cryptographie et plus précisément au système de McEliece a été proposée dans [18].

3.2.2 Prescription de la distance rang

Notation 6. — Si $g \in \mathbb{F}_q[X, \theta]$, on note L_g l'opérateur aux différences associé à g via l'application ψ définie au paragraphe 3.1.15.

De manière similaire aux codes BCH où l'on impose une distance rang en demandant que le polynôme générateur possède des puissances de racines primitives consécutives, il est possible de faire l'équivalent dans notre contexte.

Théorème 3.2.6. — *Soient m l'ordre de $\theta \in Aut(\mathbb{F}_q)$, $g \in \mathbb{F}_q[X, \theta]$ et $L_g(y) = 0$ l'équation aux différences associée. On suppose qu'il existe des entiers $n \geq \delta \geq 1$ et un élément $\beta \in \mathbb{F}_{q^s}$ tels que :*

1. *$\beta, \theta(\beta), ..., \theta^{n-1}(\beta)$ sont linéairement indépendants sur $(\mathbb{F}_q)^\theta$.*
2. *pour chaque $i \in \{0, ..., \delta - 1\}$, $L_g(\theta^i(\beta)) = 0$.*

Alors pour tout polynôme $f \in (\mathbb{F}_q)^\theta[X^m]$, c'est-à-dire dans le centre de $\mathbb{F}_q[X, \theta]$, de degré n qui est divisible à droite par g, le code $\langle g \rangle / \langle f \rangle$ est de distance minimale rang $\geq \delta + 1$, et par conséquent de distance minimale au moins $\delta + 1$.

Démonstration. — Soit c un mot du code $\langle g \rangle / \langle f \rangle$ non nul et de rang τ sur $(\mathbb{F}_q)^\theta$. Les coefficients de c forment un vecteur de longueur n : $(c_0, ..., c_{n-1}) \in \mathbb{F}_q^n$ de rang τ sur $(\mathbb{F}_q)^\theta$. Par conséquent, il existe $U \in M_{\tau \times n}((\mathbb{F}_q)^\theta)$ de rang τ et $C_1, ..., C_\tau \in \mathbb{F}_q^\tau$ linéairement indépendants sur $(\mathbb{F}_q)^\theta$ tels que :

$$(c_0, ..., c_{n-1}) = (C_1 ..., C_\tau)U. \tag{3.5}$$

D'autre part le mot de code c est un multiple à gauche, hg, de g, la multiplication dans $\mathbb{F}_q[X, \theta]$ correspondant à la composition des opérateurs aux différences, nous avons : $L_c(y) = L_h(L_g(y))$. Ainsi toute solution γ de $L_g(y) = 0$ est également une solution de $L_c(y) = 0$ et il existe une base de l'espace des solutions de $L_g(y) = 0$ sous la forme $(\beta, ..., \beta^{\delta-1}, \gamma_\delta, ..., \gamma_{k-1})$. Cela montre que :

$$(c_0,\dots,c_{n-1})\begin{pmatrix} \beta & \cdots & \theta^{\delta-1}(\beta) & \gamma_\delta & \cdots & \gamma_{k-1} \\ \theta(\beta) & \cdots & \theta^{\delta}(\beta) & \theta(\gamma_\delta) & \cdots & \theta(\gamma_{k-1}) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \theta^{n-1}(\beta) & \cdots & \theta^{n+\delta-2}(\beta) & \theta^{n-1}(\gamma_\delta) & \cdots & \theta^{n-1}(\gamma_{k-1}) \end{pmatrix} = 0.$$

Nous définissons $u_i(\beta)$ comme :

$$\forall i = 1,\dots\tau, \quad u_i(\beta) = \sum_{j=0}^{n} U_{ij}\theta^i(\beta).$$

En remplaçant $(c_0,\dots,c_{n-1})$ par l'expression 3.5, et en utilisant que les coefficients de U sont stables par θ nous obtenons :

$$(C_1,\dots,C_t)\begin{pmatrix} u_1(\beta) & \cdots & \theta^{\delta-1}(u_1(\beta)) & u_1(\gamma_\delta) & \cdots & u_1(\gamma_{k-1}) \\ u_2(\beta) & \cdots & \theta^{\delta-1}(u_2(\beta)) & u_2(\gamma_\delta) & \cdots & u_2(\gamma_{k-1}) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ u_t(\beta) & \cdots & \theta^{\delta-1}(u_t(\beta)) & u_t(\gamma_\delta) & \cdots & u_t(\gamma_{k-1}) \end{pmatrix} = 0.$$

Comme U est de rang τ et que $\beta, ..., \theta^{n-1}(\beta)$ sont linéairement indépendants sur $(\mathbb{F}_q)^\theta$ nous avons $u_1(\beta), ..., u_\tau(\beta)$ également linéairement indépendants sur $(\mathbb{F}_q)^\theta$. Les δ premières colonnes de la matrice du système précédent sont linéairement indépendantes. Si $\tau \leq \delta$ l'équation précédente n'a pas de solution non nulle. Donc la distance minimale rang de $\langle g\rangle/\langle f\rangle$ est au moins $\delta + 1$.

■

3.2.3 Mise en oeuvre du théorème

On peut penser à l'algorithme suivant pour utiliser le théorème :

Remarque 3.2.7. — Il faut garder à l'esprit que dans toute cette partie $(\mathbb{F}_q)^\theta = \mathbb{F}_{q_0}$ puisque $\theta(x) = x^{q_0}$ et $q = q_0^t$.

1. On choisit $\mathbb{F}_q$ un corps fini, $\theta \in Aut(\mathbb{F}_q)$, le degré de l'extension dans laquelle nous allons chercher nos solutions, s, et δ un entier ≥ 1.
2. On prend un élément $\beta \in \mathbb{F}_{q^s}$ et on calcule le plus grand τ tel que :

   $$\beta, ..., \theta^{\tau-1}(\beta)$$

   soient linéairement indépendants sur $(\mathbb{F}_q)^\theta$.
3. Si $\tau \geq \delta$, on trouve un opérateur aux différences, L_g, ayant pour solutions :

   $$\beta, ..., \theta^{\delta-1}(\beta)$$

   en calculant le Casoratien de ces éléments.

4. On transforme cet opérateur en un polynôme générateur $g \in \mathbb{F}_{q^s}$.
5. On calcule une borne de ce polynôme, si le degré de cette borne n est plus petit que τ on entre dans les hypothèses du théorème précédent et l'on forme le θ-code correspondant.

Le point 4 montre le point d'achoppement de cette façon de faire, en effet le polynôme générateur g que l'on obtient est a priori à coefficients dans $\mathbb{F}_{q^s}$ puisque construit en calculant le Casoratien d'éléments de $\mathbb{F}_{q^s}$. C'est ici que le lemme 3.1.22 intervient.

Nous allons calculer le plus petit sous $(\mathbb{F}_q)^\theta$-espace vectoriel stable par $\sigma(x) = x^q$ contenant $\beta, ..., \theta^{\delta-1}(\beta)$.

Notons cet espace V_β et choisissons la base suivante pour cet espace :

$$\beta, ..., \theta^{\delta-1}(\beta), \gamma_1, ..., \gamma_r.$$

En pratique pour calculer cet espace, nous ajoutons les éléments de la forme $\sigma^j(\theta^i(\beta))$ pour $1 \leq j \leq s$ et nous prenons une base sous la forme précédente.

Il convient de remplacer le point 3 de la mise de l'algorithme précédent par le point suivant :

3′. On calcule $L_g(y) = Cas(\beta, ..., \theta^{\delta-1}(\beta), \gamma_1, ..., \gamma_r, y)$. Il est à coefficients dans $\mathbb{F}_q$ et a pour solutions, en particulier, le sous espace vectoriel engendré par :

$$\beta, ..., \theta^{\delta-1}(\beta).$$

Le point 5 de l'algorithme soulève également un problème, afin de vérifier les hypothèses du théorème, il convient que le degré de la borne, n, soit plus petit ou égal à τ sinon

$$\beta, ..., \theta^{n-1}(\beta)$$

ne seront pas linéairement indépendants.

La proposition suivante montre que pour entrer dans les hypothèses du théorème nous devons avoir en réalité $n = \tau$. En gardant les mêmes notations que précédemment, nous avons :

Lemme 3.2.8. — *Soit f une borne de g, alors le degré de f est supérieur ou égal à τ.*

Démonstration. — Le polynôme f est un multiple à gauche de g, donc $f = hg$ dans $\mathbb{F}_q[X, \theta]$. En traduisant cette opération dans le monde des opérateurs aux différences, c'est-à-dire en appliquant la fonction ψ de la proposition 3.1.15, nous avons $L_f = L_h \circ L_g$ ce qui montre que β est une solution de L_f. Or, L_f est à coefficients dans $(\mathbb{F}_q)^\theta$ comme c'est un polynôme central de $\mathbb{F}_q[X, \theta]$, nous avons alors :

$$L_f(\theta^i(\beta)) = \theta^i(L_f(\beta)) = 0.$$

Ce qui montre, en particulier, que l'espace vectoriel sur $(\mathbb{F}_q)^\theta$ engendré par $\beta, ..., \tau(\beta)$ est contenu dans l'ensemble des solutions de $L_f(y) = 0$. Ainsi pour des raisons de degré $\deg(f) \leq \tau$ ∎

Nous en déduisons que pour que la condition 1 du théorème soit satisfaite nous devons avoir le degré de la borne $n = \tau$.

Par conséquent, nous pouvons vérifier si l'opérateur ayant pour solution $\beta, ..., \theta^{\tau-1}(\beta)$ est central et si ce n'est pas le cas, on peut arrêter l'algorithme et choisir un autre β.

3.2.4 Algorithme de création de codes correcteurs

Pour résumer, l'étude précédente nous mène à l'algorithme suivant :

1. On choisit $\mathbb{F}_q$ un corps fini, $\theta \in Aut(\mathbb{F}_q)$, le degré de l'extension dans laquelle nous allons chercher nos solutions, s et δ un entier ≥ 1.
2. On prend un élément $\beta \in \mathbb{F}_{q^s}$ et on calcule le plus grand τ tel que :

$$\beta, ..., \theta^{\tau-1}(\beta)$$

   soient linéairement indépendants sur $(\mathbb{F}_q)^\theta$.
3. On calcule le Casoratien de $\beta, ..., \theta^{\tau-1}(\beta)$. Si ce n'est pas un polynôme central, on stoppe l'algorithme et on choisit un autre élément β.
4. Si $\tau \geq \delta$, on calcule $L_g(y) = Cas(\beta, ..., \theta^{\delta-1}(\beta), \gamma_1, ..., \gamma_r, y)$, il est à coefficients dans $\mathbb{F}_q$ et a pour solutions, en particulier, le sous espace vectoriel engendré par :

$$\beta, ..., \theta^{\delta-1}(\beta).$$

5. On transforme cet opérateur en un polynôme générateur $g \in \mathbb{F}_q$.
6. On forme le θ-code engendré par g de longueur τ en utilisant la matrice génératrice qui découle de g de longueur le degré, n, de f.

Lorsque la borne f sera de la forme $X^n - 1$, les codes obtenus entrent dans la famille de codes étudiés par Gabidulin dans [9], cependant sa méthode de construction de ces codes était différente, il donnait en particulier la matrice de parité du code.

Voyons à présent quelques exemples.

3.2.5 Exemples

Exemple 3.2.9. — On prend $\mathbb{F}_q = \mathbb{F}_4$, $\theta(x) = x^2$ et $s = 6$. Cela signifie que nous allons choisir $\beta \in \mathbb{F}_{4^6}$ pour construire des codes sur $\mathbb{F}_4$. Notons α le générateur de $\mathbb{F}_{4^6}^*$ et w le générateur $\mathbb{F}_4^*$ donnés par Magma dans sa version 2.13. Voyons deux exemples de codes avec ces paramètres.

1. On prend $\beta = \alpha^{3688} \in \mathbb{F}_{4^6}$. Ici, nous avons $\tau = 8$, c'est-à-dire que sur $\mathbb{F}_2 = (\mathbb{F}_4)^\theta$ les éléments $\beta, \theta(\beta), \ldots, \theta^7(\beta)$ sont linéairement indépendants. C'est-à-dire que si nous obtenons un θ-code à partir de ce β, il sera de longueur $n = 8$. En utilisant le Casoratien, nous calculons $L_\beta(y) = (\theta^8 + \theta^6 + \theta^2 + 1)(y)$. Le polynôme associé $f_L = X^8 + X^6 + X^2 + 1 \in \mathbb{F}_2[X, \theta]$ est central, en effet $f \in \mathbb{F}_2[X^2]$, nous pouvons construire

un code sur $\mathbb{F}_4$ en utilisant cet élément $\beta \in \mathbb{F}_{4^6}$. Prenons $\delta = 1$, nous calculons le plus petit $\mathbb{F}_2$-espace vectoriel, V_β contenant $\{\beta\}$ qui est stable sous l'action de $\sigma\colon x \mapsto x^4$ de $\mathrm{Aut}(\mathbb{F}_{4^6}/\mathbb{F}_4)$. Une base de V_β est $\{\beta, \theta^2(\beta), \theta^4(\beta), \theta^6(\beta)\}$ (on remarque que $\sigma = \theta^2$). En utilisant le Casoratien, nous trouvons le polynôme tordu suivant $g = X^4 + \alpha^{2730}X^3 + X^2 + X + 1 = X^4 + wX^3 + X^2 + X + 1$ associé à l'opérateur aux différences qui a pour espace de solution V_β. Etant donné que la longueur du code est 8, la matrice génératrice du code est

$$\begin{pmatrix} 1 & 1 & 1 & w^2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & w & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & w^2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & w & 1 \end{pmatrix}.$$

Nous obtenons un code de paramètres $[8, 4, 4]$ sur $\mathbb{F}_4$ de rang prescrit 2. Ce code s'envoie sur un code de paramètres $[16, 8, 4]$ sur $\mathbb{F}_2$. Ce n'est pas un code de Gabidulin.

Remarque 3.2.10. — Il y a plusieurs façons d'envoyer un code issu de $\mathbb{F}_4$ sur $\mathbb{F}_2$, ici on a utilisé la commande SubfieldRepresentationCode qui écrit chaque coordonnée de $\mathbb{F}_4$ comme un vecteur de longueur 2 sur $\mathbb{F}_2$, cela double donc la longueur du code.

2. Prenons $\beta = \alpha^{1444}$. La plus longue suite linéairement indépendante sur $\mathbb{F}_2 = (\mathbb{F}_4)^\theta$ est $\beta, \theta(\beta), \ldots, \theta^{11}(\beta)$. La dimension $[\mathbb{F}_{4^6} : \mathbb{F}_2] = 12$, cela signifie que β engendre une base normale et que la borne doit forcément être $f = X^{12} - 1$ (qui est toujours une borne dans ce cas puisque l'ordre de $\theta \in \mathrm{Aut}(\mathbb{F}_{4^6}/\mathbb{F}_2)$ est 12). Le code que l'on obtient va être un code de Gabidulin. Le plus petit $\mathbb{F}_2$-espace vectoriel V_β contenant $\{\beta\}$ qui est stable par $\sigma\colon x \mapsto x^4$ de $\mathrm{Aut}(\mathbb{F}_{4^6}/\mathbb{F}_4)$ a pour base $\{\beta, \theta^2(\beta), \theta^4(\beta), \theta^6(\beta), \theta^8(\beta), \theta^{10}(\beta)\}$. En utilisant le Casoratien, nous obtenons le générateur :

$$\begin{aligned} g &= X^6 + \alpha^{1365}X^5 + \alpha^{1365}X^4 + \alpha^{1365}X^3 + \alpha^{2730}X^2 + \alpha^{1365}X + 1 \\ &= X^6 + w^2X^5 + w^2X^4 + w^2X^3 + wX^2 + w^2X + 1. \end{aligned}$$

Comme la longueur du code est 12, la matrice génératrice correspondante est :

$$\begin{pmatrix} 1 & w^2 & w & w^2 & w^2 & w^2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & w & w^2 & w & w & w & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & w^2 & w & w^2 & w^2 & w^2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & w & w^2 & w & w & w & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & w^2 & w & w^2 & w^2 & w^2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & w & w^2 & w & w & w & 1 \end{pmatrix}.$$

Nous obtenons un $[12, 6, 6]$-code sur $\mathbb{F}_4$ de rang prescrit 2 qui est un code de Gabidulin. Le code descend en un code de paramètres $[24, 12, 6]$ sur $\mathbb{F}_2$.

Exemple 3.2.11. — On se place dans $\mathbb{F}_q = \mathbb{F}_{2^4} = \mathbb{F}_{16}$, $\theta(x) = x^4$ et $s = 4$. Cela signifie que nous allons utiliser $\beta \in \mathbb{F}_{2^{16}}$ pour construire des codes sur $\mathbb{F}_{2^4}$. Nous notons α le générateur $\mathbb{F}^*_{2^{16}}$ et w le générateur $\mathbb{F}^*_{2^4}$ donnés par Magma.

1. Prenons $\beta = \alpha^{57153}$. La plus grande suite linéairement indépendante sur $\mathbb{F}_{2^2} = (\mathbb{F}_{2^4})^\theta$ est $\beta, \theta(\beta), \ldots, \theta^7(\beta)$. C'est-à-dire que si nous obtenons un θ-code par cette construction il sera de longueur $n = 8$. En utilisant le Casoratien, nous avons $L_\beta(y) = (\theta^8 - 1)(y)$. Le polynôme associé $f_L = X^8 - 1 \in \mathbb{F}_{2^2}[X, \theta]$ est central ($f \in \mathbb{F}_{2^2}[X^4]$), nous allons pouvoir construire un code $\mathbb{F}_{2^4}$ en utilisant $\beta \in \mathbb{F}_{2^{16}}$. On prend $\delta = 1$, le plus petit $\mathbb{F}_2$-espace vectoriel V_β contenant $\{\beta\}$ qui est stable par $\sigma : x \mapsto x^{16}$ de $\mathrm{Aut}(\mathbb{F}_{2^{16}}/\mathbb{F}_{16})$ est $\{\beta, \theta^2(\beta), \theta^4(\beta), \theta^6(\beta), \}$ (on remarque que $\sigma = \theta^2$). En utilisant le Casoratien, nous obtenons le polynôme générateur suivant :

$$\begin{aligned} g &= X^4 + \alpha^{17476}X^3 + \alpha^{56797}X^2 + \alpha^{39321}X + \alpha^{39321} \\ &= X^4 + w^4X^3 + w^{13}X^2 + w^9X + w^9. \end{aligned}$$

Comme la longueur du code associé est 8, nous avons la matrice génératrice suivante :

$$\begin{pmatrix} w^9 & w^9 & w^{13} & w^4 & 1 & 0 & 0 & 0 \\ 0 & w^6 & w^6 & w^7 & w & 1 & 0 & 0 \\ 0 & 0 & w^9 & w^{13} & w^4 & 1 & 0 & 0 \\ 0 & 0 & 0 & w^6 & w^6 & w^7 & w & 1 \end{pmatrix}.$$

Le code obtenu est de paramètres $[8, 4, 5]$ sur $\mathbb{F}_{16}$, tandis que la distance rang prescrite était 2, c'est un code de Gabidulin. Il s'envoie sur un code de paramètres $[32, 16, 7]$ sur $\mathbb{F}_2$.

2. $\beta = \alpha^{18575}$. La plus grande suite linéairement indépendante sur $\mathbb{F}_{2^2} = (\mathbb{F}_{2^4})^\theta$ est $\beta, ..., \theta^5(\beta)$. L'opérateur $L_\beta(y) = (\theta^6 + \theta^4 + \theta^2 + 1)(y)$ est associé à un polynôme central. Une base de V_β est $\{\beta, \theta^2(\beta), \theta^4(\beta)\}$. Le polynôme que l'on obtient est :

$$\begin{aligned} g &= X^3 + \alpha^{61166}X^2 + \alpha^{56797}X + 1 \\ &= X^3 + w^{14}X^2 + w^{13}X + 1. \end{aligned}$$

La matrice du code associé est :

$$\begin{pmatrix} 1 & w^{13} & w^{14} & 1 & 0 & 0 \\ 0 & 1 & w^7 & w^{11} & 1 & 0 \\ 0 & 0 & 1 & w^{13} & w^{14} & 1 \end{pmatrix}.$$

Nous obtenons un code de paramètres $[6, 3, 4]$ sur $\mathbb{F}_{16}$. Ce n'est pas un code de Gabidulin.

3.2.6 Tables de résultats

Les tables suivantes montrent les paramètres des codes à distance prescrite qui sont définis sur $\mathbb{F}_4$ avec $\theta(x) = x^2$. Les lignes indiquent l'extension de $\mathbb{F}_4$ dans laquelle β a été choisi. Les colonnes indiquent le rang prescrit, δ, durant la construction. Une entrée du tableau $[10, 5, 4](8)$ signifie que l'on trouve 8 polynômes de $\mathbb{F}_4[X, \theta]$ différents qui donnent

un code de paramètres $[10, 5, 4]$. Nous indiquons également par un "g" les codes de Gabidulin. On ne met dans une case que les codes ayant la distance minimale la plus grande à longueur et dimension fixées.

On remarque que l'on obtient des codes avec des paramètres identiques avec des β provenant d'extensions différentes, toutefois pour chaque extension nous ne considérons que les β qui n'appartiennent pas à un sous-corps.

	$\delta = 1$
$\mathbb{F}_4$	$\mathbf{[2, 1, 2]}_g(2)$
$\mathbb{F}_{4^2}$	$\mathbf{[4, 2, 3]}_g(4)$
$\mathbb{F}_{4^3}$	$[6, 3, 2]_g(2)$ $[6, 3, 3]_g(4)$ $\mathbf{[6, 3, 4]}_g(2)$ $\mathbf{[4, 2, 2]}(4)$
$\mathbb{F}_{4^4}$	$\mathbf{[8, 4, 4]}_g(16)$ $\mathbf{[6, 3, 3]}(8)$
$\mathbb{F}_{4^5}$	$[10, 5, 2]_g(2)$ $[10, 5, 4]_g(14)$ $\mathbf{[10, 5, 5]}_g(16)$ $[8, 4, 2](2)$ $[8, 4, 3](2)$ $\mathbf{[8, 4, 4]}(12)$

	$\delta = 1$
$\mathbb{F}_{4^6}$	$[12, 6, 3]_g(12)$ $[12, 6, 4]_g(12)$ $[12, 6, 5]_g(32)$ $\mathbf{[12, 6, 6]}_g(8)$ $[10, 5, 3]$ $\mathbf{[10, 5, 4]}(8)$ $[8, 4, 2](2)$ $[8, 4, 3](8)$ $\mathbf{[8, 4, 4]}(22)$

	$\delta = 1$
$\mathbb{F}_{4^7}$	$[14, 7, 2]_g(2)$ $[14, 7, 4]_g(14)$ $[14, 7, 5]_g(40)$ $\mathbf{[14, 7, 6]}_g(72)$ $[12, 6, 2](2)$ $[12, 6, 4](30)$ $\mathbf{[12, 6, 5]}(32)$ $[8, 4, 2](4)$ $[8, 4, 3](24)$ $\mathbf{[8, 4, 4]}(4)$ $\mathbf{[6, 3, 3]}(16)$

Les codes en gras correspondent à des codes atteignant la meilleure distance minimale possible à longueur et dimension fixées.

Les tables suivantes qui sont organisées de la même manière que les précédentes, montrent les résultats que l'on obtient sur $\mathbb{F}_8$.

	$\delta = 1$	$\delta = 2$
$\mathbb{F}_8$	$\mathbf{[3, 2, 2]}_g(3)$	$\mathbf{[3, 1, 3]}_g(3)$
$\mathbb{F}_{8^2}$	$[6, 4, 2]_g(3)$ $\mathbf{[6, 4, 3]}_g(9)$	$[6, 2, 3]_g(3)$ $\mathbf{[6, 2, 5]}_g(9)$
$\mathbb{F}_{8^3}$	$[9, 6, 3]_g(54)$ $\mathbf{[9, 6, 4]}_g(9)$ $\mathbf{[6, 4, 3]}(21)$	$[9, 3, 6]_g(54)$ $\mathbf{[9, 3, 7]}_g(9)$ $\mathbf{[6, 2, 5]}(21)$
$\mathbb{F}_{8^4}$	$[12, 8, 2]_g(3)$ $[12, 8, 3]_g(63)$ $\mathbf{[12, 8, 4]}_g(126)$ $[9, 6, 2](3)$ $\mathbf{[9, 6, 3]}(45)$	$[12, 4, 3]_g(3)$ $[12, 4, 5]_g(9)$ $[12, 4, 6]_g(54)$ $[12, 4, 7]_g(54)$ $\mathbf{[12, 4, 8]}_g(72)$ $[9, 3, 3](3)$ $[9, 3, 5](9)$ $\mathbf{[9, 3, 6]}(36)$

	$\delta = 1$	$\delta = 2$
$\mathbb{F}_{8^5}$	$[15, 10, 2]_g(5)$ $[15, 10, 3]_g(120)$ $[15, 10, 4]_g(432)$ $\mathbf{[15, 10, 5]}_g(120)$ $[12, 8, 2](3)$ $[12, 8, 3](78)$ $\mathbf{[12, 8, 4]}(144)$	$[15, 5, 3]_g$ $[15, 5, 6]_g$ $[15, 5, 7]_g$ $[15, 5, 8]_g$ $\mathbf{[15, 5, 9]}_g$ $[12, 4, 3]$ $[12, 4, 5]$ $[12, 4, 6]$ $\mathbf{[12, 4, 7]}$

Voici à présent les résultats sur $\mathbb{F}_{16}$.

	$\delta = 1$	$\delta = 2$	$\delta = 3$
$\mathbb{F}_{16}$	$[\mathbf{4}, \mathbf{3}, \mathbf{2}]_g(8)$	$[\mathbf{4}, \mathbf{2}, \mathbf{3}]_g(8)$	$[\mathbf{4}, \mathbf{1}, 4]_g(8)$
$\mathbb{F}_{16^2}$	$[\mathbf{8}, \mathbf{6}, \mathbf{3}]_g(64)$	$[8, 4, 4]_g(32)$ $[\mathbf{8}, \mathbf{4}, \mathbf{5}]_g(32)$	$[\mathbf{8}, \mathbf{2}, \mathbf{7}]_g(64)$
$\mathbb{F}_{16^3}$	$[12, 9, 2]_g(32)$ $[12, 9, 3]_g(408)$ $[\mathbf{12}, \mathbf{9}, \mathbf{4}]_g(72)$ $[8, 6, 2](16)$ $[\mathbf{8}, \mathbf{6}, \mathbf{3}](48)$	$[12, 6, 3]_g(8)$ $[12, 6, 4]_g(72)$ $[12, 6, 5]_g(136)$ $[\mathbf{12}, \mathbf{6}, \mathbf{6}]_g(296)$ $[8, 4, 3](16)$ $[8, 4, 4](40)$ $[\mathbf{8}, \mathbf{4}, \mathbf{5}](8)$	$[12, 3, 4]_g(8)$ $[12, 3, 6]_g(64)$ $[12, 3, 8]_g(152)$ $[12, 3, 9]_g(216)$ $[\mathbf{12}, \mathbf{3}, \mathbf{10}]_g(72)$ $[8, 2, 4](8)$ $[8, 2, 5](8)$ $[\mathbf{8}, \mathbf{2}, \mathbf{7}](48)$
$\mathbb{F}_{16^4}$	$[16, 12, 3]_g(256)$ $[16, 12, 4]_g(3840)$ $[\mathbf{12}, \mathbf{9}, \mathbf{3}](512)$	$[16, 8, 6]_g(368)$ $[16, 8, 7]_g(3008)$ $[\mathbf{16}, \mathbf{8}, \mathbf{8}]_g(720)$ $[12, 6, 5](192)$ $[\mathbf{12}, \mathbf{6}, \mathbf{6}](320)$	$[16, 4, 10]_g(256)$ $[16, 4, 11]_g(1536)$ $[\mathbf{16}, \mathbf{4}, \mathbf{12}]_g(2304)$ $[\mathbf{12}, \mathbf{3}, \mathbf{8}](512)$

Remarque 3.2.12. — La raison pour laquelle, on ne prend que $\delta = 1$ avec $\mathbb{F}_q = \mathbb{F}_4$ est simple. Imaginons que l'on prenne $\delta \geq 2$. Regardons V_β, le $\mathbb{F}_2$-espace vectoriel contenant en particulier $\beta, \theta(\beta)$ stable par $\sigma = \theta^2$. Soit $r = 0$ ou $r = 1$, V_β contient $\theta^{2i+r}(\beta) = \sigma^i(\theta^r(\beta))$. Ceci montre que le polynôme générateur serait de même degré que la longueur du code. C'est pour cette raison que nous ne regardons pas ce cas là.

De même lorsque $\mathbb{F}_q = \mathbb{F}_8$, il n'est pas intéressant de prendre $\delta \geq 3$.

L'exemple suivant montre deux codes ayant les mêmes paramètres, non équivalents, construits avec cette méthode, l'un étant de Gabidulin et l'autre non.

Exemple 3.2.13. — En utilisant des éléments de $\mathbb{F}_{8^8}$, nous obtenons deux codes non équivalents de paramètres $[21, 14, 6]$ définis sur $\mathbb{F}_8$, 6 étant la plus grande distance minimale connue pour ces paramètres :

1. Le code engendré par

$$g = X^7 + wX^6 + w^3X^5 + w^5X^4 + w^6X^3 + w^4X^2 + w \in \mathbb{F}_8[X, \theta]$$

où w est le générateur de $\mathbb{F}_8^*$ donné par Magma. La borne de g est :

$$f = X^{21} + X^{18} + X^{15} + X^{12} + X^9 + X^6 + X^3 + 1 \in \mathbb{F}_2[X^3].$$

Ce code n'est pas un code de Gabidulin.

2. Le code engendré par :

$$g = X^7 + wX^6 + w^3X^5 + w^4X^4 + w^5X^3 + w^3X^2 + wX + w^2 \in \mathbb{F}_8[X, \theta].$$

La borne de g est

$$f = X^{21} + 1 \in \mathbb{F}_2[X^3].$$

C'est donc un code de Gabidulin.

Voyons à présent un exemple où l'on obtient un code qui améliore la meilleure distance minimale connue sur $\mathbb{F}_8$.

Exemple 3.2.14. — Prenons $\mathbb{F}_q = \mathbb{F}_8$, $\theta(x) = x^2$ et $s = 14$. Cela signifie que nous allons utiliser des éléments de $\mathbb{F}_{8^{14}}$ pour construire des codes sur $\mathbb{F}_8$. On note α le générateur $\mathbb{F}^*_{8^{42}}$ et w le générateur $\mathbb{F}^*_8$ donnés par Magma.

On choisit :

$$\beta = \alpha^{70193}.$$

La plus grande suite qui est linéairement indépendante sur $\mathbb{F}_2 = (\mathbb{F}_8)^\theta$ est $\beta, ..., \theta^{41}(\beta)$. En utilisant le Casoratien, nous avons :

$$L_\beta(y) = \theta^{42}(y) + y.$$

Le polynôme correspondant $f = X^{42} + 1$ est central. Nous prenons $\delta = 2$. Le plus petit $\mathbb{F}_2$-espace vectoriel contenant $\{\beta, \theta(\beta)\}$ qui est stable par $\sigma(x) = x^8$ a pour dimension 28 et le polynôme tordu associé, g est :

$$g = X^{28} + w^2X^{27} + X^{26} + w^5X^{25} + w^3X^{24} + wX^{23} + w^2X^{22} + w^4X^{21}$$

$$+w^2X^{19} + X^{18} + w^5X^{17} + w^4X^{16} + wX^{15} + X^{14} + w^2X^{13} + w^4X^{12} + w^4X^{11}$$

$$+w^4X^{10} + w^5X^9 + w^5X^7 + w^6X^6 + w^5X^5 + w^5X^4 + w^6X^3 + w^4X^2 + w^6X + w.$$

Nous pouvons calculer comme d'habitude la matrice génératrice du code, nous obtenons un code θ-cyclique sur $\mathbb{F}_8$ avec les paramètres :

$$[42, 14, 21].$$

Ce code augmente de 1 la meilleure distance minimale connue jusqu'à présent pour un code sur $\mathbb{F}_8$ de longueur 42 et de dimension 14.

Une borne supérieure sur la distance minimale (ici la borne de Griesmer) est, dans ce cas, 25.

3.3 Codes BCH tordus

3.3.1 Introduction

Le but de cette section est de mettre au point une construction analogue à celle des codes BCH dans le contexte non-commutatif. En commutatif le polynôme générateur g est simplement un produit de $(X-\alpha^i)$ pour certains indices i bien choisis. Généraliser cela ici est assez difficile étant donné qu'en non-commutatif un produit de polynômes dépend de l'ordre dans lequel on effectue les multiplications. La notion correspondante va en fait être celle de plus grand commun multiple à gauche.

Afin de voir cela nous avons besoin du lemme suivant :

Lemme 3.3.1. — *Soit $\theta(x) = x^{q_0}$ un automorphisme de $\mathbb{F}_q$, avec $q_0^t = q$. Pour toute extension $\mathbb{F}_{q^s}$, de $\mathbb{F}_q$ et pour tout $\sigma \in Aut(\mathbb{F}_{q^s}/\mathbb{F}_q)$, l'application :*

$$\begin{array}{rcl} \varphi_\sigma : \mathbb{F}_{q^s}[X,\theta] & \to & \mathbb{F}_{q^s}[X,\theta] \\ \sum_{i=0}^{n} a_i X^i & \mapsto & \sum_{i=0}^{n} \sigma(a_i) X^i \end{array}$$

est un morphisme d'anneau.

Démonstration. — On note à nouveau θ l'automorphisme de $\mathbb{F}_{q^s}$ défini par $\theta(x) = x^{q_0}$. La structure additive est clairement préservée et, en ce qui concerne la structure multiplicative, nous avons de manière immédiate :

$$\varphi_\sigma(aX) = \varphi_\sigma(a)\varphi_\sigma(X).$$

Mais en non-commutatif nous sommes également tenus de vérifier que $\varphi_\sigma(Xa) = \varphi_\sigma(X)\varphi_\sigma(a)$, c'est-à-dire :

$$\sigma(\theta(a))X = \varphi_\sigma(\theta(a)X) = \varphi_\sigma(Xa) = \varphi_\sigma(X)\varphi_\sigma(a) = \theta(\sigma(a))X.$$

La condition est vérifiée étant donné que σ et θ, en tant qu'automorphismes de $\mathbb{F}_{q^s}$, commutent. ∎

Nous en déduisons le lemme suivant qui va être utile :

Lemme 3.3.2. — *Soit $f(X) = a_n X^n + ... + a_1 X + a_0 \in \mathbb{F}_q[X,\theta]$ et supposons que $a_0 \neq 0$, alors il existe une extension $\mathbb{F}_{q^s}$ telle que f soit le plus petit commun multiple à gauche de polynômes de la forme $X - \alpha^i$ où $\alpha^i \in \mathbb{F}_{q^s}$.*

Démonstration. — Il existe un corps $\mathbb{F}_{q^s}$ où se trouvent toutes les solutions de $L_f(y) = 0$. Pour chaque solution $\beta \in \mathbb{F}_{q^s}$ de $L_f(y)$, nous avons, d'après la proposition 3.1.17, $X - \frac{\theta(\beta)}{\beta}$ qui est un facteur à droite de f dans $\mathbb{F}_{q^s}[X,\theta]$. Ainsi le plus petit multiple à gauche, g, des $X - \frac{\theta(\beta)}{\beta}$ quand β parcourt l'ensemble des solutions de $L_f(y) = 0$, est aussi un facteur à droite de f. Soit σ un générateur de $Aut(\mathbb{F}_{q^s}/\mathbb{F}_q)$, σ commute avec l'extension de θ à $\mathbb{F}_{q^s}$,

donc σ envoie une solution de $L_f(y) = 0$ sur une autre solution. Cela montre que φ_σ envoie g sur lui même et par conséquent que g est à coefficients dans $\mathbb{F}_q$. Remarquons ensuite que l'opérateurL_f n'a que des solutions de multiplicité 1 comme a_0 est non nul. Etant donné que toutes les solutions de f sont également des solutions de g, le degré de g est au moins égal à celui de f, donc f et g coïncident (à une constante près).

■

Les codes BCH tordus ont été introduits dans [31] et étudiés uniquement en caractéristique 2. Ici nous présentons leur étude générale.

3.3.2 Conditions d'existence des codes BCH tordus

Définition 3.3.3. — *Soit $\theta(x) = x^{q_0}$ un automorphisme de $\mathbb{F}_q$ et $q = q_0^t$. Un **code BCH tordu** de longueur n sur $\mathbb{F}_q$ pour les paramètres entiers non nuls δ et s est un θ-code engendré par le polynôme $g \in \mathbb{F}_q[X, \theta]$ vérifiant :*

1. *$g \in \mathbb{F}_q[X, \theta]$ est le polynôme de plus petit degré divisible à droite par $X - \alpha^k$ pour $k \in \{1, ..., \delta - 1\}$ où α est un générateur de $\mathbb{F}^*_{q_0^s}$.*
2. *g a pour borne un polynôme f de degré n.*

Nous dirons qu'un tel code est un (n, q_0, t, s, δ)-code BCH tordu.

Proposition 3.3.4. — *Si $n \leq (q_0 - 1)s$ alors un (n, q_0, t, s, δ)-code est de distance minimale au moins δ.*

Démonstration. — Supposons que le code est engendré par $g \in \mathbb{F}_q[X, \theta]$ et que f soit une borne de g de degré n. Un élément $h = \sum_{i=0}^{n-1} c_i X^i \in \mathbb{F}_q[X, \theta]/\langle f \rangle$ est un mot de code si et seulement si c'est un multiple à gauche de g ou de manière équivalente si α^k est une racine de P_h, le polynôme de Jacobson introduit à la proposition 1.7.7 pour $k \in \{1, ..., \delta - 1\}$. Pour des commodités de notation, posons $[i] = \frac{q_0^i - 1}{q_0 - 1}$.
La matrice de parité du code est alors obtenue comme dans [31] :

$$\begin{pmatrix} \alpha^{[0]} & \alpha^{[1]} & \cdots & \alpha^{[\delta-1]} & \cdots & \alpha^{[n-1]} \\ (\alpha^2)^{[0]} & (\alpha^2)^{[1]} & \cdots & (\alpha^2)^{[\delta-1]} & \cdots & (\alpha^2)^{[n-1]} \\ \vdots & & & & & \vdots \\ (\alpha^{\delta-1})^{[0]} & (\alpha^{\delta-1})^{[1]} & \cdots & (\alpha^{\delta-1})^{[\delta-1]} & \cdots & (\alpha^{\delta-1})^{[n-1]} \end{pmatrix}.$$

Nous utilisons dans la suite de la démonstration la caractérisation classique de la distance minimale à l'aide des mineurs de la matrice de parité.
Tous les déterminants extraits de taille $(\delta - 1) \times (\delta - 1)$ sont non nuls si et seulement si :

$$\alpha^{[i]} \neq \alpha^{[j]}$$

pour tout $i > j \in \{0, 1, ..., n - 1\}$.

Supposons que ce ne soit pas le cas c'est-à-dire que $\alpha^{[i]} = \alpha^{[j]}$, alors :

$$\alpha^{\frac{(q_0)^i-(q_0)^j}{q_0-1}} = \alpha^{\frac{(q_0)^j\cdot\left((q_0)^{i-j}-1\right)}{q_0-1}} = 1. \tag{3.6}$$

En particulier $\alpha^{(q_0)^j\cdot\left((q_0)^{i-j}-1\right)} = 1$, implique que $q_0^{j-1} - 1$ est divisible par $q_0^s - 1$, l'ordre de α. Donc $i - j = ms$ et d'après la relation précédente $q_0 - 1$ divise

$$\frac{q_0^{m\cdot s} - 1}{q_0^s - 1} = \sum_{r=0}^{m-1} (q_0)^{s\cdot k}.$$

Cela veut dire que $q_0 - 1$ divise m, donc $i - j$ est un multiple de $(q_0 - 1)s$, mais alors $i - j < n \leq (q_0 - 1)s$, ce qui n'est pas possible.

■

3.3.3 Mise en oeuvre algorithmique

Soit α un générateur du groupe multiplicatif de $\mathbb{F}_{q_0^s}$. Un polynôme g est divisible à droite par $X - \alpha^i$, si et seulement si la solution β_i de $\theta(y) - \alpha^i(y) = 0$ est aussi solution de l'opérateur aux différences $L_g(y) = 0$ associé à g. Le fait que $g \in \mathbb{F}_q[X, \theta]$ soit le polynôme tordu de plus petit degré divisible à droite par $X - \alpha^i$ pour $i \in \{1, ..., \delta - 1\}$ est équivalent au fait que l'espace des solutions de $L_g(y) = 0$ contienne $\beta_1, ..., \beta_{\delta-1}$. D'après le lemme 3.1.22, $L_g(y)$ est défini sur $\mathbb{F}_q$ lorsque son espace de solutions est stable par σ un générateur de $Aut(\mathbb{F}_{q_0^s}/\mathbb{F}_q)$. L'algorithme suivant donne la méthode de fabrication de codes BCH tordus.

1. On choisit α un générateur de $\mathbb{F}^*_{q_0^s}$.
2. Pour tout $i \in \{1, ..., \delta - 1\}$, on calcule β_i tel que :

$$\frac{\theta(\beta_i)}{\beta_i} = \alpha^i.$$

   .
3. On détermine le plus petit espace vectoriel sur $\mathbb{F}_{q_0}$ qui contient $\beta_1, ..., \beta_{\delta-1}$ et qui est stable sous l'action de $\sigma(x) = x^q$. On le note V_g.
4. En utilisant le Casoratien, on calcule l'opérateur aux différences qui a pour espace de solutions V_g, on note $g \in \mathbb{F}_q[X, \theta]$ le polynôme associé.
5. On calcule une borne, f, pour g. Si le degré n de f vérifie :

$$n \leq (q_0 - 1)s$$

   alors g va engendrer un code BCH tordu dont on peut minorer la distance minimale par δ.
6. On forme la matrice génératrice comme usuellement.

Remarque 3.3.5. — Le point 1 de l'algorithme montre que l'on a plusieurs possibilités pour le choix des β_i. En réalité ces choix différents mènent au même code.

Typiquement, nous devons trouver β dans une extension de $\mathbb{F}_{q_0}$ tel que $\frac{\theta(\beta)}{\beta} = \alpha$, cela se traduit simplement par une équation polynomiale :

$$\beta^{q_0-1} = \alpha \tag{3.7}$$

puisque $\theta(x) = x^{q_0}$. Notons j un générateur de $\mathbb{F}_{q_0}^*$, si $\beta_0 \in \mathbb{F}_{q_0^N}$ est une solution de l'équation 3.7 alors l'ensemble de toutes les solutions de l'équation est :

$$\{j^0\beta_0, j\beta_0, ..., j^{q_0-2}\beta_0\}.$$

Soit β_i solution de $\frac{\theta(\beta_i)}{\beta_i} = \alpha^i$ pour $i = 1...\delta - 1$. L'ensemble de tous les β_i que l'on peut choisir est donc :

$$\{(j^{r_1}\beta_0, j^{r_2}\beta_0^2, ..., j^{r_{\delta-1}}\beta_0^{\delta-1}),\ (r_1, r_2, ...r_{\delta-1}) \in \{0, ..., q_0 - 2\}\}.$$

Regardons le Casoratien de ces élements pour voir de quelle manière il dépend du choix des r_i.

$$\mathrm{Cas}(j^{r_1}\beta_0, \ldots, j^{r_{\delta-1}}\beta_0^{\delta-1}, y) = \begin{vmatrix} j^{r_1}\beta_0 & \ldots & j^{r_{\delta-1}}\beta_0^{\delta-1} & y \\ \theta(j^{r_1}\beta_0) & \ldots & \theta(j^{r_{\delta-1}}\beta_0^{\delta-1}) & \theta(y) \\ \theta^2(j^{r_1}\beta_0) & \ldots & \theta^2(j^{r_{\delta-1}}\beta_0^{\delta-1}) & \theta^2(y) \\ \ldots & \ldots & \ldots & \ldots \\ \theta^{\delta-1}(j^{r_1}\beta_0) & \ldots & \theta^{\delta-1}(j^{r_{\delta-1}}\beta_0^{\delta-1}) & \theta^{\delta-1}(y) \end{vmatrix}.$$

Comme j^{r_i} est dans $(\mathbb{F}_q)^\theta$, nous avons :

$$Cas(j^{r_1}\beta_0, \ldots, j^{r_{\delta-1}}\beta_0^{\delta-1}, y) = j^{r_1}j^{r_2}...j^{r_{\delta-1}}Cas(\beta_0, \beta_0^2, ..., \beta_0^{\delta-1}, y).$$

Donc, quelque soit le choix des $\beta_1, ..., \beta_{\delta-1}$ de l'étape 1 de l'algorithme, les codes obtenus sont les mêmes à une constante près.

Remarque 3.3.6. — Il est possible que g soit divisible à droite par $X - \alpha^i$ pour $i \geq \delta$, il est par conséquent intéressant de calculer Δ le plus grand entier tel que g soit divisible à droite par :

$$X - \alpha, ..., X - \alpha^{\Delta-1}.$$

Il est en effet tout à fait possible que Δ soit strictement plus grand que le δ que l'on a choisi au début et dans ce cas on tombe sur un meilleur minorant de la distance minimale.

Voyons tout de suite des exemples de mise en oeuvre de cet algorithme.

Exemple 3.3.7. — On se place dans $\mathbb{F}_q = \mathbb{F}_{2^3}$, $\theta : x \mapsto x^2$ et $s = 9$. Cela veut dire que nous allons utiliser des éléments $\alpha \in \mathbb{F}_{2^9}$ pour construire des codes sur $\mathbb{F}_{2^3}$. Notons γ le générateur de $\mathbb{F}_{2^9}^*$ et w le générateur de $\mathbb{F}_{2^3}^*$ donnés par Magma. On prend $\alpha = \gamma^{433}$ et $\delta = 2$. Le plus petit $\mathbb{F}_2 = (\mathbb{F}_{2^3})^\theta$ espace vectoriel V_{α,α^2} contenant $\{\alpha, \alpha^2\}$ qui est stable par

$\sigma: x \mapsto x^8$ dans $\mathrm{Aut}(\mathbb{F}_{2^9}/\mathbb{F}_3)$ a pour base $\{\alpha, \gamma^{483}, \gamma^{410}, \gamma^{179}\}$. En utilisant le Casoratien, nous calculons :

$$L_{\alpha,\gamma^{483},\gamma^{410},\gamma^{179}}(y) = \theta^4(y) + w^2\theta^3(y) + w\theta^2(y) + w\theta(y) + y.$$

Le polynôme tordu associé est $g = X^4+w^2X^3+wX^2+wX+1 \in \mathbb{F}_{2^3}[X,\theta]$ c'est le générateur du code BCH tordu que nous allons construire. La borne de g est $f = X^6+X^3+1 \in \mathbb{F}_2[X^3]$. Donc la longueur du code va être 6 est la matrice génératrice est :

$$\begin{pmatrix} 1 & w & w & w^2 & 1 & 0 \\ 0 & 1 & w^2 & w^2 & w^4 & 1 \end{pmatrix}.$$

On obtient un code de paramètres $[6, 2, 5]$ sur $\mathbb{F}_8$.

3.3.4 Tableaux de résultats

Les tables qui suivent montrent les caractéristiques des codes à distance prescrite définis sur $\mathbb{F}_4$ pour $\theta(x) = x^2$. Les lignes indiquent le corps où α a été choisi, les colonnes indiquent la distance minimale δ qui a été prescrite. Une entrée $[6, 3, 3](8)$ signifie que l'on a trouvé pour ces paramètres 8 polynômes tordus différents qui donnent un code de paramètres $[6, 3, 3]$.

	$\delta = 2$	$\delta = 3$	$\delta = 4$	$\delta = 5$	$\delta = 6$	$\delta = 7$
$\mathbb{F}_{2^6}$	$[6,3,3](6)$ $[6,3,4](6)$	$[6,1,6](1)$ $[6,2,4](1)$	$[6,1,6](1)$	$[6,1,6](1)$		
$\mathbb{F}_{2^8}$	$[8,4,4](20)$ $[6,3,3](8)$	$[8,1,8](1)$ $[6,1,4](1)$	$[8,1,8](3)$			
$\mathbb{F}_{2^{10}}$	$[10,5,4](24)$ $[10,5,5](24)$ $[\mathbf{10},\mathbf{6},\mathbf{3}](2)$ $[\mathbf{8},\mathbf{4},\mathbf{4}](12))$	$[10,1,10](1)$ $[10,4,4](1)$	$[10,1,10](3)$	$[10,1,10](3)$	$[10,1,10](3)$	$[10,1,10](3)$
$\mathbb{F}_{2^{12}}$	$[12,6,3](12)$ $[12,6,4](18)$ $[12,6,5](54)$ $[\mathbf{12},\mathbf{6},\mathbf{6}](12)$ $[12,7,3](6)$ $[\mathbf{12},\mathbf{7},\mathbf{4}](12)$ $[\mathbf{12},\mathbf{8},\mathbf{3}](6)$ $[10,5,3](6)$ $[\mathbf{10},\mathbf{5},\mathbf{4}](18)$ $[8,4,3](12)$ $[\mathbf{8},\mathbf{4},\mathbf{4}](18)$	$[\mathbf{12},\mathbf{1},\mathbf{12}](1)$ $[\mathbf{12},\mathbf{2},\mathbf{8}](1)$ $[\mathbf{12},\mathbf{3},\mathbf{4}](1)$ $[\mathbf{10},\mathbf{1},\mathbf{6}](1)$ $[10,2,4](1)$ $[\mathbf{10},\mathbf{3},\mathbf{4}](1)$ $[8,1,4](1)$ $[8,2,4](1)$ $[8,2,5](1)$ $[8,3,4](1)$	$[\mathbf{12},\mathbf{1},\mathbf{12}](3)$ $[12,2,6](2)$ $[12,2,8](3)$ $[\mathbf{12},\mathbf{2},\mathbf{9}](4)$ $[\mathbf{12},\mathbf{4},\mathbf{6}](2)$	$[\mathbf{12},\mathbf{1},\mathbf{12}](3)$ $[12,2,6](2)$ $[12,2,8](3)$ $[\mathbf{12},\mathbf{2},\mathbf{9}](3)$ $[\mathbf{12},\mathbf{4},\mathbf{6}](2)$	$[\mathbf{12},\mathbf{1},\mathbf{12}](3)$ $[12,2,8](1)$ $[\mathbf{12},\mathbf{2},\mathbf{9}](4)$	$[\mathbf{12},\mathbf{1},\mathbf{12}](3)$ $[\mathbf{12},\mathbf{2},\mathbf{8}](1)$
$\mathbb{F}_{2^{14}}$	$[14,7,4](24)$ $[14,7,5](84)$ $[\mathbf{14},\mathbf{7},\mathbf{6}](132)$ $[12,6,4](30)$ $[\mathbf{12},\mathbf{6},\mathbf{5}](48)$ $[8,4,3](24)$ $[\mathbf{8},\mathbf{4},\mathbf{4}](8)$ $[\mathbf{6},\mathbf{3},\mathbf{3}](8)$	$[14,1,14](1)$ $[14,3,8](2)$ $[14,4,6](2)$ $[14,6,4](1)$	$[\mathbf{14},\mathbf{1},\mathbf{14}](3)$ $[14,3,8](2)$ $[\mathbf{14},\mathbf{3},\mathbf{10}](4)$ $[14,4,6](2)$ $[\mathbf{14},\mathbf{4},\mathbf{8}](4)$	$[\mathbf{14},\mathbf{1},\mathbf{14}](3)$ $[14,3,8](2)$ $[\mathbf{14},\mathbf{3},\mathbf{10}](4)$ $[\mathbf{14},\mathbf{4},\mathbf{6}](2)$	$[14,1,14](3)$ $[14,3,8,1]$	$[14,1,14](3)$ $[14,3,8](1)$

Voici à présent quelques codes sur $\mathbb{F}_8$.

	$\delta = 2$	$\delta = 3$	$\delta = 4$	$\delta = 5$
$\mathbb{F}_{8^2}$	$[\mathbf{6},\mathbf{4},\mathbf{3}](18)$	$[\mathbf{6},\mathbf{2},\mathbf{5}](12)$ $[\mathbf{6},\mathbf{3},\mathbf{4}](3)$	$[\mathbf{6},\mathbf{2},\mathbf{5}](9)$ $[\mathbf{6},\mathbf{1},\mathbf{6}](3)$	$[\mathbf{6},\mathbf{1},\mathbf{6}](3)$
$\mathbb{F}_{8^3}$	$[9,6,3](108)$ $[\mathbf{9},\mathbf{6},\mathbf{4}](18)$ $[\mathbf{6},\mathbf{3},\mathbf{4}](18)$	$[9,3,6](60)$ $[\mathbf{9},\mathbf{3},\mathbf{7}](12)$ $[9,4,5](12)$ $[\mathbf{9},\mathbf{4},\mathbf{6}](3)$ $[\mathbf{6},\mathbf{2},\mathbf{5}](18)$	$[\mathbf{9},\mathbf{1},\mathbf{9}](6)$ $[9,2,6](6)$ $[\mathbf{9},\mathbf{2},\mathbf{8}](6)$ $[9,3,6](24)$ $[\mathbf{9},\mathbf{3},\mathbf{7}](3)$ $[\mathbf{9},\mathbf{4},\mathbf{5}](3)$	$[\mathbf{9},\mathbf{1},\mathbf{9}](3)$ $[\mathbf{9},\mathbf{2},\mathbf{6}](6)$
$\mathbb{F}_{8^4}$	$[12,8,3](132)$ $[\mathbf{12},\mathbf{8},\mathbf{4}](183)$ $[\mathbf{9},\mathbf{6},\mathbf{3}](54)$	$[12,4,5](12)$ $[12,4,6](60)$ $[\mathbf{12},\mathbf{4},\mathbf{7}](48)$ $[12,5,6](21)$ $[\mathbf{12},\mathbf{5},\mathbf{7}](12)$ $[12,6,4](12)$ $[\mathbf{12},\mathbf{7},\mathbf{4}](3)$ $[\mathbf{12},\mathbf{8},\mathbf{4}](72)$ $[9,3,5](12)$ $[\mathbf{9},\mathbf{3},\mathbf{6}](21)$ $[9,4,4](6)$ $[\mathbf{9},\mathbf{5},\mathbf{4}](3)$	$[\mathbf{12},\mathbf{1},\mathbf{12}](6)$ $[12,2,6](3)$ $[12,2,8](6)$ $[\mathbf{12},\mathbf{2},\mathbf{10}](9)$ $[12,3,6](6)$ $[12,3,8](3)$ $[\mathbf{12},\mathbf{3},\mathbf{9}](18)$ $[12,4,7](9)$ $[\mathbf{12},\mathbf{4},\mathbf{8}](3)$ $[12,5,5](3)$ $[\mathbf{12},\mathbf{5},\mathbf{6}](12)$ $[\mathbf{12},\mathbf{6},\mathbf{5}](3)$	$[\mathbf{12},\mathbf{1},\mathbf{12}](3)$ $[12,2,6](3)$ $[12,2,8](6)$ $[\mathbf{12},\mathbf{2},\mathbf{10}](3)$ $[12,3,6](9)$ $[12,3,8](6)$ $[\mathbf{12},\mathbf{3},\mathbf{9}](3)$ $[12,4,6](3)$ $[\mathbf{12},\mathbf{5},\mathbf{6}](3)$

L'exemple suivant présente un code BCH tordu qui dépasse la meilleure distance minimale connue jusqu'à présent.

Exemple 3.3.8. — On prend $\mathbb{F}_q = \mathbb{F}_4$, $\theta(x) = x^2$ et $s = 40$. Cela signifie que nous allons utiliser des éléments de $\mathbb{F}_{4^{20}}$ pour construire des codes sur $\mathbb{F}_4$. On appelle γ le générateur de $\mathbb{F}_{4^{20}}^*$ et w le générateur de $\mathbb{F}_4^*$ donné par Magma.

Soit

$$\alpha = \gamma^{6971}.$$

Le plus petit $\mathbb{F}_2 = (\mathbb{F}_4)^\theta$-espace vectoriel V_α contenant $\{\alpha\}$ qui est stable par $\sigma(x) = x^4$ a pour dimension 17. Le polynôme générateur correspondant est :

$$g = X^{17} + wX^{16} + wX^{14} + X^{13} + w^2X^{12} + X^{11} + wX^9 + X^8 + wX^7 + w^2X^6 + X^5 + wX + w.$$

La borne de g est $f = X^{40} + 1$.

On obtient un code de paramètres $[40, 23, 10]$ sur $\mathbb{F}_4$.

Ce code améliore de 1 la meilleure distance minimale connue jusqu'à présent pour un code de longueur 40 et de dimension 23.

La borne supérieure pour la distance minimale, dans ce cas la borne de Griesmer, est 13.

3.3.5 Décodage des codes BCH tordus

Les codes que nous venons de voir sont construits par analogie avec les codes BCH classiques et il est possible d'adapter l'algorithme usuel pour les décoder dans ce cadre non-commutatif. L'algorithme de décodage des BCH commutatifs est présenté dans [32] au paragraphe 6.7.

En utilisant les notations de la définition 3.3.3, nous avons un (n, q_0, t, s, δ)-code BCH tordu que nous appelons $\mathcal{C}$. On suppose que ce code peut corriger Γ erreurs.

Considérons le mot de code $c \in \mathcal{C}$ et l'erreur $e(x) = e_{i_1}x^{i_1} + ... + e_{i_\gamma}x^{i_\gamma}$ avec bien sûr $\gamma \leq \Gamma$.

Soit $c' = c + e = \sum_{j=0}^{n} c'_j x^j$ le mot reçu. La question est de retrouver e connaissant c'.

1. D'après la proposition 1.7.5, le reste dans la division à droite de e par $X - \alpha^i$ pour $i = 1...\delta - 1$ est :

$$A_i = \sum_{j=0}^{n-1} e_j (\alpha^i)^{[j]}.$$

où $\beta^{[j]} = \beta^{\frac{q_0^i - 1}{q_0 - 1}}$. Il est possible de calculer A_i connaissant uniquement c' étant donné que le reste de la division euclidienne à droite de e par $X - \alpha^i$ est le même que le reste de la division euclidienne de c' par $X - \alpha^i$. Donc :

$$A_i = \sum_{j=0}^{n-1} c'_j (\alpha^i)^{[j]}.$$

On définit le polynôme syndrome de e par :

$$S(z) = \sum_{k=1}^{\delta-1} A_i z^{i-1} \in \mathbb{F}_{q^s}[z].$$

2. On définit le polynôme localisateur par :

$$\sigma(z) = \prod_{k=1}^{\gamma} (1 - \alpha^{[i_k]} z)$$

et le polynôme d'évaluation par :

$$w(z) = \sum_{l=1}^{\gamma} e_{i_l} \alpha^{[i_l]} \prod_{k \neq l} (1 - \alpha^{[i_k]} z).$$

3. Connaître $\sigma(z)$ nous permet de trouver $[i_k] = \frac{q_0^{i_k}-1}{q_0-1}$ mod (q^s-1). Pour ce faire nous devons trouver $[i_1], ..., [i_\gamma]$ tels que $\sigma(\alpha^{-[i_1]}) = ... = \sigma(\alpha^{-[i_\gamma]}) = 0$. Cette recherche peut être faite en calculant $\sigma(x)$ pour tout $x \in \mathbb{F}_{q^s}$. Connaissant $[i_k]$ et $w(z)$, nous pouvons trouver les coefficients e_{i_k} puisque :

$$e_{i_k} = \alpha^{-[i_k]} w(\alpha^{-[i_k]}) \prod_{l \neq k} (1 - \alpha^{[i_l]-[i_k]})$$

pour $k \in \{1...\gamma\}$.

4. Nous utilisons l'algorithme d'Euclide appliqué aux polynômes $S(z)$ et $z^{\delta-1} \in \mathbb{F}_{q^s}[z]$. Nous arrêtons dès que nous trouvons le premier reste de degré plus petit que Γ, et nous avons

$$u(z)z^{\delta-1} + v(z)S(z) = r(z).$$

Comme dans l'algorithme classique de décodage des BCH, on peut prouver que $\sigma(z) = v(z)/v(0)$ et $w(z) = r(z)/v(0)$. Et si nous connaissons σ et w, nous avons vu que nous pouvons reconstruire l'erreur e et trouver le mot envoyé c.

Chapitre 4

Codes modules

Dans le chapitre 2, nous avons étudié largement les codes correcteurs construits comme des idéaux d'un anneau quotient de polynômes non-commutatifs. Ceci vient du fait que le quotient $\mathbb{F}_q[X,\theta]/I$ où I est un idéal à gauche de $\mathbb{F}_q[X,\theta]$ a une structure d'anneau si et seulement si I est un idéal bilatère.

Cependant, lorsque I n'est pas forcément bilatère, même si le quotient n'a pas une structure d'anneau, c'est un $\mathbb{F}_q[X,\theta]$-module à gauche. Grâce à cette remarque on peut voir un sous-module à gauche de $\mathbb{F}_q[X,\theta]/I$ comme un code correcteur avec la correspondance classique qui à un polynôme associe le n-uplet de ses coefficients.

Cette généralisation a été étudiée très récemment dans [29].

Le fait de s'affranchir de la condition bilatère va considérablement simplifier l'obtention d'un code correcteur à partir du polynôme générateur. Nous allons pouvoir notamment nous permettre de considérer des anneaux non-commutatifs plus généraux avec l'ajout d'une dérivation. Dans le cadre des codes idéaux il n'était pas forcément évident de caractériser le centre d'un anneau de polynômes non-commutatifs avec une dérivation et donc le calcul d'une borne était compromis. Nous allons voir que dans le cadre des codes modules ce calcul s'implémente très bien. Cela nous permettra d'élargir à nouveau la famille de codes obtenus et nous verrons que l'ajout d'une dérivation nous permettra dans certains cas de trouver de nouveaux codes.

Nous allons en premier lieu préciser notre méthode de construction pour les codes modules sans dérivation puis avec dérivation. Dans le cas de $\mathbb{F}_q[X,\theta,\delta]$ il va falloir faire quelques calculs notamment pour exprimer $X^n a$. Puis nous présenterons quelques tableaux de résultats et nous analyserons les données obtenues. Enfin nous verrons que le cadre défini est assez agréable pour rechercher les duaux de certains codes et en particulier caractériser les codes auto-duaux. Enfin nous verrons que l'utilisation des codes modules permet de généraliser à nouveau les techniques du chapitre précédent, nous donnerons par exemple un code correcteur de paramètres $[41, 13, 21]$ sur $\mathbb{F}_8$ qui améliore de 1 la meilleure distance minimale connue auparavant pour ces paramètres, ce code ne pouvait être obtenu sans les codes modules.

4.1 Codes-modules sans dérivation

On se place dans $\mathbb{F}_q[X,\theta]$. On choisit f un polynôme de degré n, alors $\mathbb{F}_q[X,\theta]/\langle f\rangle_g$ est un $\mathbb{F}_q[X,\theta]$-module à gauche. Le quotient $\mathbb{F}_q[X,\theta]/\langle f\rangle_g$ est également un $\mathbb{F}_q[X,\theta]$-module à gauche. Grâce au théorème de correspondance des sous modules d'un module quotient, nous savons que les sous-modules à gauche de $\mathbb{F}_q[X,\theta]/\langle f\rangle_g$ sont de la forme $\mathbb{F}_q[X,\theta]g$ où g est un diviseur à droite de f. Via l'application T définie au chapitre précédent qui convertit tous les restes possibles dans la division à droite par f en n-uplets, on obtient un code correcteur.

On ne va pas en pratique fixer f en premier mais plutôt g. Soit $g \in \mathbb{F}_q[X,\theta]$ sous la forme suivante :

$$g = g_0 + g_1X + ...g_rX^r$$

où $g_r \neq 0$. Alors pour tout $n \geq r$ il existe un multiple à gauche de g de degré n, notons le f. Le code module correspondant au plongement de $\mathbb{F}_q[X,\theta]g$ dans $\mathbb{F}_q[X,\theta]/\langle f\rangle_g$ est engendré en tant que $\mathbb{F}_q[X,\theta]$-espace vectoriel par les éléments de la forme :

$$X^ig,\ \forall i \in \{0...n-r-1\}$$

de la même manière que dans la définition 2.4 du chapitre 2. Ainsi la matrice génératrice a également la forme suivante :

$$\begin{pmatrix} g_0 & \cdots & g_{r-1} & g_r & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \cdots & \theta(g_{r-1}) & \theta(g_r) & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \theta^{n-r-1}(g_0) & \cdots & \theta^{n-r-1}(g_{r-1}) & \theta^{n-r-1}(g_r) \end{pmatrix}.$$

Le code correcteur engendré par cette matrice est de longueur n, de dimension $n-r$.

Remarque 4.1.1. — La majeure différence avec le chapitre précédent sur les codes-idéaux est qu'ici nous n'avons pas besoin d'avoir la forme explicite de f. Le code est uniquement déterminé par le générateur g et le degré.

Résumons cela :

Définition 4.1.2. — *Soit f de degré n, un **code θ-module** est un sous $\mathbb{F}_q[X,\theta]$-module à gauche engendré par un diviseur à droite de f, g de $\mathbb{F}_q[X,\theta]/\langle f\rangle_g$. Si g est de degré r et si d est la distance minimale alors on dit que le code a pour paramètres $[n, n-r, d]$. On notera le code $C_n(g)$.*

Notation 7. — Nous appelerons θ-codes les codes correcteurs construits aux chapitres 2 qui sont donc inclus dans les codes modules.

Remarque 4.1.3. — Soit n et r fixés, il y a q^r choix pour le polynôme g de degré r à coeffcients dans $\mathbb{F}_q$. En effet, on le suppose unitaire étant donné que $C_n(g)$ et $C_n(\alpha g)$ sont égaux avec $\alpha \in (\mathbb{F}_q)^*$, il suffit donc de choisir les r coefficients restants dans $\mathbb{F}_q$. Ainsi, il y a au plus q^r codes θ-modules de longueur n et de dimension $n-r$. Bien sûr, certains peuvent être équivalents.

Voyons tout de suite quelques exemples qui illustrent la méthode de construction d'un code θ-module.

Exemple 4.1.4. — On se place dans $\mathbb{F}_8[X]$, c'est-à-dire que pour cet exemple l'automorphisme θ est l'identité. On note α le générateur de $\mathbb{F}_8^*$ fourni par Magma.

On prend le polynôme générateur g suivant :

$$X^7 + \alpha^4 X^6 + X^5 + \alpha^5 X^4 + \alpha^5 X^2 + X + \alpha^4.$$

On prend la longueur du code n égale à 11.

Une matrice génératrice du code $C_{11}(g)$ est de la forme :

$$\begin{pmatrix} \alpha^4 & 1 & \alpha^5 & 0 & \alpha^5 & 1 & \alpha^4 & 1 & 0 & 0 & 0 \\ 0 & \alpha^4 & 1 & \alpha^5 & 0 & \alpha^5 & 1 & \alpha^4 & 1 & 0 & 0 \\ 0 & 0 & \alpha^4 & 1 & \alpha^5 & 0 & \alpha^5 & 1 & \alpha^4 & 1 & 0 \\ 0 & 0 & 0 & \alpha^4 & 1 & \alpha^5 & 0 & \alpha^5 & 1 & \alpha^4 & 1 \end{pmatrix}.$$

La distance minimale de ce code est 7. Ceci est la meilleure distance minimale possible pour un code de longueur 11 et de dimension 4 sur $\mathbb{F}_8$.

Exemple 4.1.5. — On se place dans $\mathbb{F}_4[X, \theta]$ où $\theta(x) = x^2$. On note α le générateur donné par Magma. On considère le polynôme générateur suivant :

$$g = X^5 + X^3 + \alpha X^2 + \alpha X + \alpha^2.$$

Une matrice du code génératrice $C_{10}(g)$ est de la forme :

$$\begin{pmatrix} \alpha^2 & \alpha & \alpha & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha^2 & \alpha & \alpha & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \alpha^2 & \alpha & \alpha & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha^2 & \alpha & \alpha & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \alpha^2 & \alpha & \alpha & 1 & 0 & 1 \end{pmatrix}.$$

C'est un code de paramètres $[10, 5, 5]$ sur $\mathbb{F}_4$ qui atteint également la meilleure distance minimale possible.

Nous verrons dans le paragraphe 3 des tableaux de résultats qui vont nous permettre de comparer les codes θ-modules aux meilleurs codes connus, nous verrons qu'ils apportent quelque chose par rapport aux θ-codes. Mais tout de suite étudions ce qui se passe lorsque nous faisons intervenir une dérivation.

4.2 Codes-modules avec dérivation

4.2.1 Introduction

Le fait de ne plus avoir besoin de calculer un multiple central du polynôme générateur g va nous permettre de travailler dans le cadre le plus général où l'anneau de polynômes tordu possède une dérivation.

Nous rappelons la règle de calcul suivante :

Définition 4.2.1. — *Soit $\mathbb{F}_q$ un corps fini, on note $\mathbb{F}_q[X, \theta, \delta]$ l'anneau de polynômes non-commutatif où la multiplication est définie par la règle simple suivante :*

$$\forall a \in \mathbb{F}_q,\ Xa = \theta(a)X + \delta(a).$$

Les différentes dérivations existantes dans un corps fini, ainsi que les premières propriétés de l'anneau $\mathbb{F}_q[X, \theta, \delta]$ ont été étudiées dans le paragraphe 7 du chapitre 1. Tout ce que l'on a vu dans le paragraphe précédent est également vrai dans ce cadre là. Nous pouvons étant donné un polynôme générateur g de degré r et un entier $n \geq r$, définir une base de notre code correcteur avec les polynômes suivants :

$$X^i g(X),\ \forall i \in \{0...n-r-1\}.$$

La matrice génératrice s'obtiendra en transformant les coefficients de ces polynômes en n-uplet que l'on mettra en ligne.

Il convient d'expliciter les coefficients de $X^i g(X)$.

4.2.2 Calcul de $X^i g(X)$

Etant donné qu'en toute généralité, θ et δ ne commutent pas, nous avons besoin de la notation suivante. On suppose l'anneau $\mathbb{F}_q[X, \theta, \delta]$ fixé.

Définition 4.2.2. — *Soit $a \in \mathbb{F}_q$, on note $S_{i,j}(a)$ la somme des C_i^j termes obtenus en appliquant θ $i-j$ fois et δ j fois.*

Exemple 4.2.3. —Nous avons :

$$S_{4,3}(a) = \theta(\delta^3(a)) + \delta(\theta(\delta^2(a))) + \delta^2(\theta(\delta(a))) + \delta^3(\theta(a))$$

où la puissance désigne bien l'itération pour la loi de composition.

Proposition 4.2.4. — *Soit $a \in \mathbb{F}_q$. Dans l'anneau $\mathbb{F}_q[X, \theta, \delta]$, nous avons la formule suivante :*

$$X^i a = \sum_{j=0}^{i} S_{i,j}(a) X^{i-j}. \tag{4.1}$$

Pour plus de détails, on pourra consulter [21].

Exemple 4.2.5. — En utilisant la proposition précédente, on a directement :

$$X^2a = \theta^2(a)X^2 + [\theta(\delta(a)) + \delta(\theta(a))]X + \delta^2(a).$$

Soit le polynôme :

$$g = g_0 + g_1X + ... + g_rX^r.$$

Nous pouvons expliciter $X^ig(X)$, en effet par associativité :

$$X^ig(X) = (X^ig_0) + (X^ig_1)X... + (X^ig_r)X^r.$$

En utilisant la proposition précédente, nous avons :

$$X^ig(X) = \sum_{j=0}^{i} S_{i,j}(g_0)X^{i-j} + \sum_{j=0}^{i} S_{i,j}(g_1)X^{i-j+1} + ... + \sum_{j=0}^{i} S_{i,j}(g_r)X^{i-j+r}.$$

Pour mieux lire le polynôme que l'on obtient on peut regrouper les termes en fonction de la puissance de X correspondante :
Coefficient de X^0 : $S_{i,i}(g_0)$.
Coefficient de X^1 : $S_{i,i-1}(g_0) + S_{i,i}g_1$.
Coefficient de X^2 : $S_{i,i-2}(g_0) + S_{i,i-1}g_1 + S_{i,i}(g_2)$.
Coefficient de X^{i+r} : $S_{i,i-(i+r)}(g_0) + ... + S_{i,0}(g_r)$.
On peut unifier ces expressions en adoptant la convention suivante :

$$S_{i,j} = 0, \ \forall j \notin \{0, ..., i\}.$$

Définition 4.2.6. —*Soit* $(k, r, i) \in \mathbb{N}^3$ *et* $g = g_0 + g_1X + ... + g_rX^r$ *un polynôme de degré* r*, on pose :*

$$T_i^k(g) = \sum_{j=0}^{r} S_{i,i+j-k}(g_j). \tag{4.2}$$

On peut résumer le calcul précédent avec la formule :

Proposition 4.2.7. — *Dans l'anneau* $\mathbb{F}_q[X, \theta, \delta]$*, nous avons :*

$$X^ig(X) = \sum_{k=0}^{i+r} T_i^k(g)X^k. \tag{4.3}$$

4.2.3 Exemple de codes tordus avec dérivation

Etant donné que nous avons l'expression sous forme polynomiale des mots de code $X^i g(X)$ et que nous savons que ces polynômes pour i allant de 0 à $n-r-1$ engendrent le code, nous en déduisons l'expression de la matrice génératrice :

$$M = (T_i^k)_{0\leq i\leq n-r-1,\ 0\leq k\leq n-1}. \tag{4.4}$$

Toutes ces expressions étant explicites, nous pouvons à partir d'un polynôme g, avoir la matrice génératrice du code engendré par g.

Voyons un exemple :

Exemple 4.2.8. — On désigne toujours par α le générateur de $\mathbb{F}_4^*$ donné par Magma. On se place dans $\mathbb{F}_4[X,\theta,\delta]$ où $\theta(x) = x^2$ et $\delta(x) = \alpha x^2 + \alpha x$ qui est bien une θ-dérivation avec :

$$\delta(0) = \delta(1) = 0$$

$$\delta(\alpha) = \delta(\alpha^2) = \alpha.$$

La vérification exhaustive qu'il s'agit d'une θ-dérivation est très rapide comme le corps ne contient que 4 éléments.

On s'intéresse au polynôme :

$$g(X) = X^5 + \alpha^2 X^2 + X + \alpha^2.$$

On prend $n = 16$, la matrice génératrice du code $C_{16}(g)$ est la suivante :

$$\begin{pmatrix}
\alpha^2 & 1 & \alpha^2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\alpha & \alpha & \alpha^2 & \alpha & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\alpha & 1 & 1 & 0 & \alpha^2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\alpha & \alpha^2 & 1 & 1 & \alpha & \alpha & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\alpha & 1 & \alpha & 1 & \alpha^2 & 1 & \alpha^2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\alpha & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha & \alpha^2 & \alpha & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
\alpha & 1 & 0 & 0 & 0 & 0 & 1 & 0 & \alpha^2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
\alpha & \alpha^2 & 1 & 0 & 0 & 0 & 0 & 1 & \alpha & \alpha & 0 & 0 & 1 & 0 & 0 & 0 \\
\alpha & 1 & \alpha & 1 & 0 & 0 & 0 & 0 & \alpha^2 & 1 & \alpha^2 & 0 & 0 & 1 & 0 & 0 \\
\alpha & \alpha^2 & \alpha^2 & \alpha^2 & 1 & 0 & 0 & 0 & \alpha & \alpha & \alpha^2 & \alpha & 0 & 0 & 1 & 0 \\
\alpha & 1 & 0 & 0 & \alpha & 1 & 0 & 0 & \alpha & 1 & 1 & 0 & \alpha^2 & 0 & 0 & 1
\end{pmatrix}.$$

La distance minimale est 4 ce qui est la meilleure distance minimale possible pour un code correcteur sur $\mathbb{F}_4$ de longueur 16 et de dimension 11.

Exemple 4.2.9. — On note α le générateur de $\mathbb{F}_8^*$ donné par Magma. On se place dans $\mathbb{F}_8[X,\theta,\delta]$ où $\theta(x) = x^2$ et la θ-dérivation δ est définie par :

$$\delta(0) = \delta(1) = 0$$

$$\delta(\alpha) = \delta(\alpha^3) = \alpha$$
$$\delta(\alpha^2) = \delta(\alpha^6) = \alpha^5$$
$$\delta(\alpha^4) = \delta(\alpha^5) = \alpha^6.$$

On considère le polynôme g suivant :

$$g(X) = X^4 + \alpha^4 X^3 + \alpha^4 X^2 + \alpha^4.$$

On prend $n = 10$ la matrice génératrice du code correspondant est :

$$\begin{pmatrix} \alpha^4 & 0 & \alpha^4 & \alpha^4 & 1 & 0 & 0 & 0 & 0 & 0 \\ \alpha^6 & \alpha & \alpha^6 & \alpha^5 & \alpha & 1 & 0 & 0 & 0 & 0 \\ \alpha^5 & \alpha^6 & \alpha^3 & \alpha & 1 & \alpha^2 & 1 & 0 & 0 & 0 \\ \alpha^6 & \alpha^2 & \alpha^6 & \alpha^5 & \alpha^2 & \alpha^4 & \alpha^4 & 1 & 0 & 0 \\ \alpha^5 & 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^5 & \alpha & 1 & 0 \\ \alpha^6 & \alpha^3 & 0 & \alpha^3 & \alpha^3 & \alpha^2 & 0 & 1 & \alpha^2 & 1 \end{pmatrix}.$$

Le code est de paramètres $[10, 6, 4]$ ce qui réalise la meilleure distance minimale possible sur $\mathbb{F}_8$.

4.2.4 Cas particulier où θ et δ commutent

L'introduction de la θ-dérivation complique assez largement les calculs, cela est principalement dû au fait que δ et θ ne commutent pas en général. Voyons un cas particulier dans lequel les formules mises en jeu sont beaucoup plus simples.

On se place dans $\mathbb{F}_4$ muni de $\theta(x) = x^2$, on choisit la θ-dérivation suivante :

$$\delta(0) = \delta(1) = 0$$
$$\delta(\alpha) = \delta(\alpha^2) = 1.$$

Dans ce cadre particulier δ et θ commutent, plus précisément :

$$\theta(\delta(x)) = \delta(x) = \delta(\theta(x)) \tag{4.5}$$

puisque δ est à valeurs dans $(\mathbb{F}_4)^\theta$.

Remarquons également que :

$$\delta^k(x) = 0, \ \forall k \geq 2.$$

Proposition 4.2.10. — *Nous avons les règles de calcul suivantes :*
- $S_{i,0}(a) = \theta^i(a)$.
- $S_{i,1}(a) = i\delta(a)$.
- $\forall k \geq 2, \ S_{i,k}(a) = 0$.

Démonstration. — Le premier point est la définition de $S_{i,j}$.
Pour la seconde assertion, il suffit de remarquer que $S_{i,1}(a)$ est la somme des i termes de la forme :

$$\theta^j \circ \delta \circ \theta^{i-1-j}(a) = \theta^{i-1} \circ \delta = \delta(a)$$

pour $j \in \{0...i-1\}$. Le dernier point découle de 4.5.

■

A présent, il est possible de donner une expression plus explicite des coefficients de $X^i g(X)$.

Proposition 4.2.11. —*Soit $g(X) = g_0 + g_1 X + ... + g_r X^r$, avec la notation :*

$$X^i g(X) = \sum_{k=0}^{i+r} T_i^k(g) X^k$$

nous avons :

$$T_i^k(g) = \theta^i(g_{k-i}) + i\delta(g_{k-i+1})$$

avec la convention $g_j = 0,\ \forall j \notin \{0, ..., r\}$.

Démonstration. — Par définition :

$$T_i^k(g) = \sum_{j=0}^{r} S_{i,i+j-k}(g_j).$$

D'après le point 3 de la proposition 4.2.10 tous les termes de la somme sont nuls sauf éventuellement quand $j = k - i$ ce qui donne le terme $S_{i,0}(g_{k-i}) = \theta^i(g_{k-i})$ et quand $j = k - i + 1$ correspondant à $S_{i,1}(g_{k-i+1}) = i\delta(g_{k-i+1})$. ■

Proposition 4.2.12. — *Avec les notations précédentes la matrice génératrice du code est de la forme :*

$$\begin{pmatrix} g_0 & \cdots & g_{r-1} & g_r & 0 & \cdots & 0 \\ \delta(g_0) & \theta(g_0)+\delta(g_1) & \cdots & \theta(g_{r-1})+\delta(g_r) & \theta(g_r) & \cdots & 0 \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \cdots & (n-r-1)\delta(g_0) & \theta^{n-r-1}(g_0)+(n-r-1)\delta(g_1) & \cdots & \theta^{n-r-1}(g_{r-1})+(n-r-1)\delta(g_r) & \theta^{n-r-1}(g_r) \end{pmatrix}$$

Exemple 4.2.13. — On travaille dans $\mathbb{F}_4[X, \theta, \delta]$ avec $\theta(x) = x^2$ et $\delta(x) = x^2 + x$.

On prend le polynôme générateur suivant :

$$g(X) = X^7 + \alpha^2 X^5 + \alpha X^4 + \alpha^2 X^3 + \alpha^2 X^2 + \alpha.$$

On choisit $n = 12$, la matrice génératrice du code est :

$$\begin{pmatrix} \alpha & 0 & \alpha^2 & \alpha^2 & \alpha & \alpha^2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & \alpha^2 & 1 & \alpha^2 & \alpha^2 & \alpha & \alpha & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & \alpha^2 & \alpha^2 & \alpha & \alpha^2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \alpha^2 & 1 & \alpha^2 & \alpha^2 & \alpha & \alpha & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \alpha & 0 & \alpha^2 & \alpha^2 & \alpha & \alpha^2 & 0 & 1 \end{pmatrix}.$$

La distance minimale de ce code de longueur 12 et de dimension 5 est 6, ce qui est la meilleure distance minimale possible sur $\mathbb{F}_4$.

4.3 Résultats

On peut voir un tableau comparatif des différents codes obtenus dans [29].

En introduisant les codes modules, puis les codes modules avec dérivation, nous élargissons strictement nos familles de codes correcteurs. C'est ce que nous allons voir avec ces quelques exemples sur $\mathbb{F}_4$.

On se place sur $\mathbb{F}_4[X,\theta]$, si l'on prend $\theta(x) = x$ on retrouve des polynômes commutatifs. Montrons que le fait de pouvoir choisir $\theta(x) = x^2$ donne de nouveaux codes par rapport au monde des polynômes commutatifs.

Exemple 4.3.1. — On se place dans $\mathbb{F}_4[X, Id]$. Le meilleur code obtenu pour un générateur de degré 6 et une longueur 12 est un code de paramètres $[12, 6, 5]$.

Par contre si on se place dans $\mathbb{F}_4[X,\theta]$ où $\theta(x) = x^2$, on trouve un code de distance minimale strictement meilleure et qui atteint la meilleure distance minimale possible, 6.

Un tel code est par exemple engendré par le polynôme :

$$g(X) = \alpha^2 X^6 + \alpha X^5 + \alpha X^4 + \alpha X^2 + X + 1.$$

Une matrice génératrice est :

$$\begin{pmatrix} 1 & 1 & \alpha & 0 & \alpha & \alpha & \alpha^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & \alpha^2 & 0 & \alpha^2 & \alpha^2 & \alpha & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & \alpha & 0 & \alpha & \alpha & \alpha^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & \alpha^2 & 0 & \alpha^2 & \alpha^2 & \alpha & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & \alpha & 0 & \alpha & \alpha & \alpha^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & \alpha^2 & 0 & \alpha^2 & \alpha^2 & \alpha \end{pmatrix}.$$

De la même façon, l'introduction d'une dérivation va élargir encore strictement la famille de codes correcteurs que l'on regarde.

Exemple 4.3.2. — Sur $\mathbb{F}_4[X,\theta]$ le meilleur code que l'on obtient de longueur 15 et de dimension 8 est de distance minimale 5. Ce qui n'est pas optimal comme la plus grande distance possible est 6 d'après le site http ://www.codetables.de/.

Cette distance est atteinte si l'on travaille dans $\mathbb{F}_4[X,\theta,\delta]$ avec $\delta(x) = \alpha(x^2 + x)$. En effet avec :

$$g(X) = x^7 + \alpha X^6 + \alpha X^4 + \alpha^2 X^2 + \alpha^2 X + 1$$

nous obtenons un code sur $\mathbb{F}_4$ de paramètres $[12, 8, 6]$ de matrice génératrice :

$$\begin{pmatrix} 1 & \alpha^2 & \alpha^2 & 0 & \alpha & 0 & \alpha & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^2 & 0 & \alpha & \alpha & \alpha^2 & \alpha & \alpha^2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha & \alpha & \alpha & 1 & 1 & 0 & 1 & \alpha & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 1 & 1 & \alpha^2 & 1 & 1 & 0 & \alpha^2 & \alpha^2 & 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha & \alpha^2 & 1 & \alpha^2 & \alpha & 1 & 1 & \alpha & 0 & \alpha & 1 & 0 & 0 & 0 \\ 0 & \alpha & 1 & \alpha & \alpha^2 & 0 & \alpha^2 & 1 & \alpha^2 & \alpha^2 & \alpha & \alpha^2 & 1 & 0 & 0 \\ 0 & \alpha & \alpha^2 & \alpha^2 & 1 & \alpha & \alpha & \alpha & \alpha^2 & 0 & 0 & 1 & \alpha & 1 & 0 \\ 0 & \alpha & 1 & 0 & \alpha & \alpha^2 & 1 & 1 & 1 & \alpha & 0 & 0 & \alpha^2 & \alpha^2 & 1 \end{pmatrix}.$$

Les tableaux de résultats présentés en annexe sont construits de la façon suivante : en ligne nous avons la longueur du code et en colonne le degré du polynôme générateur. Le résultat à l'intersection est la meilleure distance minimale obtenue. Pour des longueurs trop importantes les résultats ne sont bien sûr pas exhaustifs.

En annexe 1, on trouvera les codes modules sur $\mathbb{F}_2$.

En annexe 2 ,des codes sur $\mathbb{F}_4$ avec des polynômes générateurs dans l'anneau commutatif $\mathbb{F}_4[X]$.

En annexe 3, le polynôme générateur se trouvera à présent dans $\mathbb{F}_4[X,\theta]$ où $\theta(x) = x^2$.

En annexe 4, on prendra g dans $\mathbb{F}_4[X,\theta,\delta]$ avec $\delta(\alpha) = \alpha$.

Enfin en annexe 5, le polynôme générateur sera à coefficients dans $\mathbb{F}_4[X,\theta,\delta]$ avec $\delta(\alpha) = 1$.

4.4 Codes modules rang et codes modules BCH

Dans le chapitre 3, nous avons étudié des θ-codes dont on pouvait prescrire le rang, et la distance minimale. En mettant en oeuvre les outils développés dans ce chapitre, nous pouvons nous intéresser à la généralisation du chapitre 3. On peut s'affanchir du calcul de la borne du polynôme dans la plupart des cas, ainsi nous allons obtenir des codes dont la longueur varie plus librement et par conséquent obtenir plus de codes.

4.4.1 Codes-modules dont le rang est prescrit

L'algorithme du chapitre 3 peut se modifier de la manière suivante :

1. On choisit un corps fini, $\mathbb{F}_q$, θ un automorphisme de $\mathbb{F}_q$, $\delta \geq 1$ qui va prescrire la distance minimale et s un entier qui sera le degré de l'extension dans laquelle on va aller chercher nos éléments.
2. Soit $\beta \in \mathbb{F}_{q^s}$, on calcule le plus grand entier τ tel que :
$$\beta, ..., \theta^{\tau-1}(\beta)$$
soient linéairement indépendants sur $(\mathbb{F}_q)^\theta$.
3. On détermine le plus petit $(\mathbb{F}_q)^\theta$-espace vectoriel, V_β stable par $\sigma(x) = x^q$ et contenant :
$$\beta, ..., \theta^{\delta-1}(\beta).$$
4. On calcule le Casoratien de cet espace que l'on convertit en polynôme, g, de $\mathbb{F}_q[X,\theta]$.
5. Ce polynôme engendre un code-module de longueur n pour tout $\deg(g) - 1 \leq n \leq \tau$ dont on a la matrice génératrice usuelle.

Il y a plusieurs intérêts à considérer cette généralisation. Tout d'abord nous ne sommes plus tenus de vérifier si l'opérateur aux différences ayant pour solutions $\beta, ..., \theta^{\tau-1}(\beta)$ est central ce qui fait gagner en rapidité au procédé. Si jamais il n'était pas central, l'algorithme se poursuit donc nous obtenons plus de codes. La longueur des codes obtenus n'est plus nécessairement un multiple de l'ordre de θ en tant qu'endomorphisme de $\mathbb{F}_q$, en particulier

nous allons obtenir des codes de longueur impaire sur $\mathbb{F}_4$. Nous avons également plusieurs choix de longueur possibles pour un même polynôme générateur g tout en gardant notre prescription sur la distance minimale.

Voyons tout de suite 3 exemples :

Exemple 4.4.1. — On prend $\mathbb{F}_q = \mathbb{F}_4$, $s = 7$, et $\theta(x) = x^2$. Le polynôme :

$$g = X^7 + X^5 + X^4 + \alpha X^3 + \alpha^2 X^2 + X + \alpha$$

est le polynôme générateur d'un code module sur $\mathbb{F}_4$ de paramètres $[13, 6, 6]$, 6 étant la meilleure distance minimale possible pour un code ayant des paramètres. Ce code n'est pas un θ-code puisque sa longueur est impaire.

Exemple 4.4.2. — On note α le générateur de $\mathbb{F}_8^*$ donné par Magma, $\theta(x) = x^2$ et $s = 5$. Le polynôme :

$$g = \alpha^2 + X + \alpha X^2 + \alpha^6 X^3 + \alpha^2 X^4 + X^5$$

engendre un code de paramètres $[12, 7, 5]$. Ce code n'est pas non plus un θ-code qui pouvait être trouvé par les méthodes du chapitre 3, même si dans ce cas-là la longueur 12 est bien un multiple de l'ordre de θ en tant qu'endomorphisme de $\mathbb{F}_8$.

Exemple 4.4.3. — Enfin nous obtenons un nouveau code qui augmente de 1 la meilleure distance minimale connue précédemment. Ce code est défini sur $\mathbb{F}_8$, $\theta(x) = x^2$, et $s = 14$. Le polynôme générateur du code est :

$$\begin{aligned} g = {} & X^{28} + w^2X^{27} + X^{26} + w^5X^{25} + w^3X^{24} + wX^{23} + w^2X^{22} + w^4X^{21} \\ & + w^2X^{19} + X^{18} + w^5X^{17} + w^4X^{16} + wX^{15} + X^{14} + w^2X^{13} + w^4X^{12} + w^4X^{11} \\ & + w^4X^{10} + w^5X^9 + w^5X^7 + w^6X^6 + w^5X^5 + w^5X^4 + w^6X^3 + w^4X^2 + w^6X + w. \end{aligned}$$

Nous obtenons un code de paramètres : $[41, 13, 21]$ ce qui améliore de 1 la meilleure distance minimale connue jusqu'à présent.

On remarque que ce polynôme est le même que celui du chapitre 3 qui avait permis de trouver un code de paramètres $[42, 14, 21]$ qui améliorait aussi la meilleure distance minimale connue de 1, en effet il correspond au même élément $\beta \in \mathbb{F}_{4^{14}}$ mais le fait d'avoir relaxé nos contraintes sur f et son degré n, nous permet de former ce nouveau code module issu du précédent.

4.4.2 Codes-modules BCH

Tout comme nous venons de voir les codes modules dont le rang est prescrit, il est possible de généraliser la partie du chapitre 3 qui traite des codes tordus BCH avec minoration de la distance minimale. Cette généralisation est étudiée dans [29].

Si l'on se réfère à l'algorithme mis en place dans le chapitre 3, nous pouvons omettre la partie calcul de la borne de g. La seule condition sur la longueur du code dont il faut tenir compte est $n \leq (q_0 - 1)s$.

L'algorithme devient donc le suivant en reprenant les notations introduites dans le paragraphe 3 du chapitre 3.

1. On choisit α un générateur de $\mathbb{F}_{q_0^s}^*$.
2. Pour tout $i \in \{1, ..., \delta - 1\}$, on calcule β_i tel que :
$$\frac{\theta(\beta_i)}{\beta_i} = \alpha^i.$$
3. On détermine le plus petit espace vectoriel sur $\mathbb{F}_{q_0}$ qui contient $\beta_1, ..., \beta_{\delta-1}$ et qui est stable sous l'action de $\sigma(x) = x^q$. On le note V_g.
4. En utilisant le Casoratien, on calcule l'opérateur aux différences qui a pour espace de solutions V_g, on note $g \in \mathbb{F}_q[X, \theta]$ le polynôme associé.
5. On choisit un longueur de code n, vérifiant :
$$\deg(g) + 1 \leq n \leq (q_0 - 1)s$$
alors g va engendrer un code module BCH dont on peut minorer la distance minimale par δ.
6. On forme la matrice génératrice comme usuellement.

Dans ce cadre là , nous obtenons des codes BCH qui ne pouvent être obtenus uniquement avec l'algorithme du chapitre 3.

Exemple 4.4.4. — On prend $\beta = w^{11}$ un générateur de $\mathbb{F}_{2^{12}}^*$ où w est le générateur de $\mathbb{F}_{2^{12}}^*$ donné par Magma, $\theta(x) = x^2$ et nous choisissons $\delta = 2$. Le polynôme générateur g correspondant est :
$$g = X^6 + \alpha^2 X^5 + \alpha X^4 + \alpha X^2 + X + \alpha^2$$
où $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$. Ici $q_0 = 2$ et $s = 12$ donc nous pouvons choisir $n \leq 12$ pour longueur, avec bien sûr $n > 6$ quand même puisque 6 est le degré du polynôme générateur. Prenons $n = 10$, en formant la matrice génératrice, nous obtenons un code module BCH de paramètres $[10, 4, 6]$ sur $\mathbb{F}_4$, 6 étant la meilleure distance minimale possible pour un code de longueur 10 et une dimension 4.

La borne de g est $f = X^{12} + 1$ ce qui signifie que le code que l'on vient de considérer ne pouvait pas être obtenu par la construction du chapitre 3.

Voyons un peu comment se comporte la distance minimale des codes engendrés par un même générateur g lorsque l'on fait varier la longueur du code. Prenons des codes sur $\mathbb{F}_2$ puisque le phénomène est très général et n'est pas lié au monde non-commutatif.

Exemple 4.4.5. — On se place dans $\mathbb{F}_2$ et on considère le polynôme :
$$g = X^{10} + X^9 + X^8 + X^6 + X^5 + X^3 + 1.$$

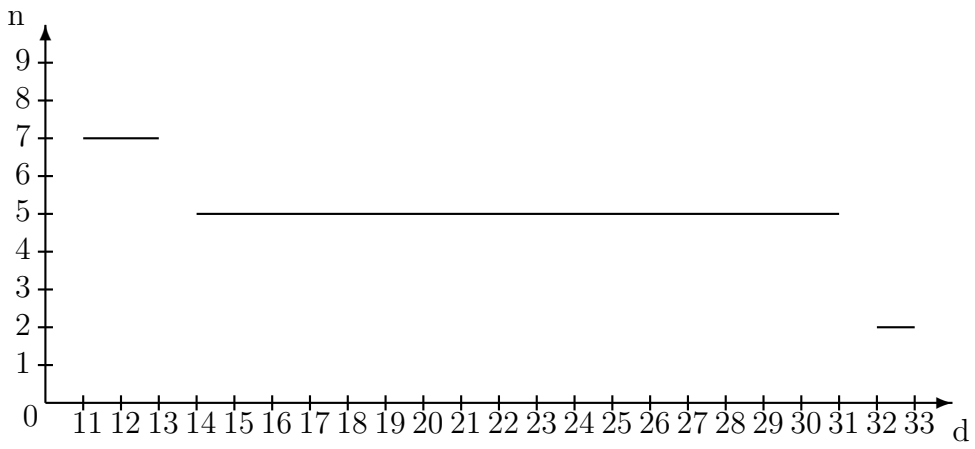
Ce polynôme a en particulier pour racine :
$$\{\beta, \beta^2, \beta^3, \beta^4\}$$

où β le générateur de $\mathbb{F}_{32}^*$ donné par Magma.

C'est-à-dire que si on choisit n tel que $\beta, ..., \beta^{n-1}$ soient distincts alors notre code aura bien au moins 5 comme distance minimale. Etant donné que β vit dans $\mathbb{F}_{32}$, tous les choix de n inférieur ou égal à 31 conviennent.

Si l'on choisit $n > 31$, on ne peut rien garantir.

Voilà un graphique donnant les différentes distances minimales du code en fonction de la longueur, la dimension du code étant toujours sa longueur moins 10 (le degré de g).



Comme annoncé la distance minimale vaut 5 jusqu'à $n = 31$ puis chute à 2 à partir de $n = 32$.

4.5 Dualité

Nous avons déjà discuté brièvement de la dualité pour des codes θ-centraux, il est à nouveau possible de regarder cela dans le cadre des codes θ-modules.

Ce sujet est traité de manière complète dans [29], rapelons-en ici les principaux résultats :

Nous avons vu dans le chapitre 2 que le dual d'un code θ-cyclique est également un code θ-cyclique. De manière plus générale, on se pose la question : quand est-ce que le dual d'un code module est un code module ? Le théorème suivant montre que le cas des codes θ-cycliques reflète presque la généralité.

Théorème 4.5.1. — *Soit $k \leq n$ des entiers, $g \in \mathbb{F}_q[X, \theta]$ de degré $n - k$ avec un terme constant non nul et $\mathcal{C}$ le code module de longueur n engendré par g. Le dual euclidien $\mathcal{C}^\perp$ de $\mathcal{C}$ est un code module engendré par un polynôme de degré k avec un terme constant non nul si et seulement si il existe $h = h_0 + ... + h_k X^k \in \mathbb{F}_q[X, \theta]$ et $c \in \mathbb{F}_q^*$ tel que $gh = X^n - c$. Dans ce cas le polynôme générateur de $\mathcal{C}^\perp$ est donné par :*

$$g^\perp = \sum_{i=0}^{k} \theta^i(h_{k-i}) X^i$$

et $g^\perp$ est un diviseur à gauche de $X^n - \theta^{k-n}(\frac{1}{c})$.

La preuve de ce théorème est présentée dans [29], elle utilise notamment le corps des fractions à droite, $\mathbb{F}_q(X,\theta)$, de $\mathbb{F}_q[X,\theta]$.

La matrice génératrice de $\mathcal{C}^\perp$ étant la matrice de parité du code $\mathcal{C}$, la matrice H suivante est la matrice de parité de $\mathcal{C}$:

$$H = \begin{pmatrix} h_{n-r} & \cdots & \theta^{n-r-1}(h_1) & \theta^{n-r}(h_0) & 0 & \cdots & 0 \\ 0 & \theta(h_{n-r}) & \cdots & \cdots & \theta^{n-r+1}(h_0) & \cdots & 0 \\ 0 & \ddots & \ddots & & & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 & \\ 0 & \cdots & 0 & \theta^{r-1}(h_{n-r}) & \cdots & \theta^{n-2}(h_1) & \theta^{n-1}(h_0) \end{pmatrix}.$$

Exemple 4.5.2. — Soit $g = X^2 + \alpha X + 1 \in \mathbb{F}_4[X,\theta]$, nous avons la relation suivante :

$$X^3 - \alpha = g(X + \alpha).$$

Le théorème précédent nous dit alors que le dual du code module de paramètres $[3,1,3]$ engendré par g est un code module engendré par $g^\perp = 1 + \alpha^2$. La matrice de parité qui est la matrice génératrice de $\mathcal{C}^\perp$ est :

$$H = \begin{pmatrix} 1 & \alpha^2 & 0 \\ 0 & 1 & \alpha \end{pmatrix}.$$

Le code $\mathcal{C}^\perp$ est un code de paramètres $[3,2,2]$ sur $\mathbb{F}_4$.

Nous pouvons également trouver les codes modules auto-duaux.

En effet si l'on prend la forme générale de la matrice génératrice d'un code module engendré par g de longueur n avec le degré de g, k tel que $2k = n$, on a une base de notre code module sous la forme :

$$c_1 = (g_0, ..., g_k, 0, ..., 0)$$
$$c_2 = (0, \theta(g_0), ..., \theta(g_k), ..., 0)$$
$$...$$
$$c_k = (0, ..., 0, \theta^{k-1}(g_0), ..., \theta^{k-1}(g_k)).$$

On peut écrire explicitement les relations que l'on a en demandant que pour tout i et j dans $\{1, ..., k\}$, on a $< c_i, c_j >= 0$. En remarquant que certaines relations comme $< c_2, c_3 >= 0$ sont les mêmes que $\theta(< c_1, c_2 >) = 0$. Il suffit donc de vérifier pour savoir si $\mathcal{C}$ est auto-dual que $< c_1, c_i >= 0$ pour tout $i \in \{1, ..., k\}$, c'est-à-dire :

$$\forall l \in \{1, ..., k\}, \ \sum_{i=0}^{l} \theta^{k-l}(g_i) g_{i+k-l} = 0. \tag{4.6}$$

Il est alors tout à fait possible d'utiliser les bases de Gröbner pour chercher systématiquement nos codes auto-duaux. L'article [29] trouve un code de paramètres $[56, 28, 15]$ sur $\mathbb{F}_4$ auto-dual qui bat le record précédent de [10].

Remarque 4.5.3. — Il est tout à fait possible de regarder le dual hermitien comme défini dans le chapitre 2 et l'on obtient un théorème très similaire à celui au dessus, voir [29].

Chapitre 5

Codes correcteurs multivariés

L'objectif de ce chapitre est de généraliser la construction des codes correcteurs tordus vue au chapitre 2. Nous allons ici adapter la construction précédente avec un anneau de polynômes multivariés. Une étude de codes correcteurs dans ce contexte multivarié mais en commutatif a été faite dans l'article [24]. Ici nous allons étudier des codes correcteurs qui seront vus comme des idéaux à gauche de :

$$\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$$

où l'anneau $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$ est un anneau de polynômes à plusieurs variables non-commutatif et I un idéal bilatère. La difficulté en plusieurs variables est qu'il n'y a pas, a priori, de base naturelle au quotient $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$. Les bases de Gröbner répondent à ce problème. Dans le théorème 5.1.9 nous adaptons cet outil au cas non-commutatif dans lequel on travaille. Puis nous adapterons la notion de borne d'un polynôme qui était à la base de notre méthode de construction de codes correcteurs au cas multivarié en introduisant la notion de borne d'un idéal, voir la définition 5.1.20, dont nous donnerons une méthode de calcul. Nous aurons alors tous les outils pour fabriquer nos codes correcteurs. L'utilisation des bases de Gröbner nous donnera facilement la longueur et la dimension du code. Nous verrons ensuite un algorithme basé sur des divisions d'un monôme par un idéal représenté par une base de Gröbner et une méthode pour construire la matrice génératrice sous forme générique de nos codes correcteurs, dans la proposition 5.3.3. Nous verrons quelques exemples détaillés de cette construction et des tableaux de résultats. Enfin, nous dirons un mot sur les codes multivariés modules en utilisant le chapitre précédent.

5.1 Etude d'un anneau de Ore multivarié

Nous allons commencer par définir notre anneau de polynômes tordus multivariés, puis nous introduirons les principaux outils qui vont servir à la construction de codes correcteurs, notamment l'adaptation des bases de Gröbner au cadre non-commutatif. Enfin nous parlerons de degré d'un idéal qui généralise la notion de degré d'un polynôme et nous définirons la borne d'un idéal.

5.1.1 Définition

On se place dans $\mathbb{F}_q$ un corps fini de caractéristique p tel que $p^r = q$. Soit $n \geq 2$, on choisit n automorphismes de $\mathbb{F}_q$, $\theta_1, ..., \theta_n$, non nécessairement distincts. On définit de manière ensembliste :

$$\mathbb{F}_q[X_1^{\theta_1}, ..., X_n^{\theta_n}] = \{ \sum_{i_1,...,i_n} a_{i_1,...,i_n} X_1^{i_1} ... X_n^{i_n},\ a_{i_1,...,i_n} \in \mathbb{F}_q\}. \tag{5.1}$$

Cet ensemble est celui des polynômes à n indéterminées à coefficients dans l'anneau $\mathbb{F}_q$. Afin d'alléger les notations, on appellera cet anneau $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$ et un élément générique sera noté :

$$\sum_{\alpha} a_\alpha X^\alpha$$

où α est un multi-indice.

On va munir cet ensemble d'une structure d'anneau non commutatif. On garde l'addition usuelle mais la multiplication est définie par la règle simple suivante :

$$\forall a \in \mathbb{F}_q,\ \forall i \in \{1, ..., n\},\ X_i a = \theta_i(a) X_i. \tag{5.2}$$

On étend cette règle par associativité et distributivité. On suppose que les variables X_i commutent. La multiplication devient alors bien définie et de manière plus précise :

$$(\sum_{\alpha} a_\alpha X^\alpha)(\sum_{\beta} b_\beta X^\beta) = \sum_{\alpha,\beta} a_\alpha \theta^\alpha(b_\beta) X^{\alpha+\beta}.$$

On utilise ici la notation suivante : si $\alpha = (\alpha_1, ..., \alpha_n)$ alors $\theta^\alpha = \theta_1^{\alpha_1} ... \theta_n^{\alpha_n}$ où la loi utilisée est la composition des automorphismes.

On a donc défini un **anneau de polynômes à plusieurs variables non commutatif**, $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$. Voyons quelques propriétés de cet anneau.

Proposition 5.1.1. — *L'anneau $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$ est unitaire, intègre et ses éléments inversibles sont les inversibles de $\mathbb{F}_q$.*

Démonstration. — On peut voir l'intégrité en utilisant le degré total et en remarquant que le degré total d'un produit est égal à la somme des degrés totaux de chacun des facteurs. La caractérisation des inversibles de cet anneau est également évidente. ∎

Par analogie avec le cas à une variable, on va étudier les codes correcteurs qui sont des idéaux à gauche de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$ où I est un idéal bilatère de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$. Pour que ce quotient ait une structure d'anneau, il convient que I soit un idéal bilatère. Si un idéal est engendré par des éléments centraux, il est en particulier bilatère. C'est pour cette raison que l'étude des éléments centraux de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$ nous intéresse.

Proposition 5.1.2. — *On a l'inclusion suivante :*

$$\{ \sum_{i_1,...,i_n} a_{i_1,...,i_n} X_1^{i_1|<\theta_1>|} ... X_n^{i_n|<\theta_n>|},\ a_{i_1,...,i_n} \in \bigcap_{i=1}^{n} (\mathbb{F}_q)^{\theta_i} \} \subset Z(\mathbb{F}_q[\underline{X}^{\underline{\theta}}]). \tag{5.3}$$

où $Z(\mathbb{F}_q[\underline{X}^{\underline{\theta}}])$ désigne le centre de l'anneau $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$ et $|<\theta_i>|$ l'ordre de l'automorphisme θ_i.

Démonstration. — Il suffit de voir par distributivité et associativité que les éléments dans l'ensemble du membre de gauche commutent avec les constantes et les X_i. Ceci est immédiat à vérifier.

■

Cela signifie que certains éléments centraux ont une forme particulièrement simple qui généralise assez naturellement le cas à une variable. On nommera par la suite ces éléments centraux particuliers les polynômes **super-centraux**. Lorsque nous travaillerons avec des idéaux bilatères, nous les chercherons très souvent engendrés par des polynômes super-centraux. L'inclusion de la proposition précédente est en générale stricte.

On va être amené à travailler avec des idéaux et des quotients dans des anneaux à plusieurs indéterminées. Dans le cas commutatif, pour de tels calculs, l'utilisation des bases de Gröbner est incontournable. Nous allons voir dans le paragraphe suivant que les principales propriétés des bases de Gröbner s'adaptent dans notre cas.

5.1.2 Bases de Gröbner en non-commutatif

Nous allons dans un premier temps rappeler brièvement les principaux éléments de construction d'une base de Gröbner dans le cadre commutatif puis nous verrons comment adapter cela au cadre non-commutatif.

Un théorème fondamental pour ce qui va suivre est le théorème de Hilbert qui nous dit que $\mathbb{K}[X_1, ..., X_n]$ est noethérien, c'est-à-dire :

Théorème 5.1.3. — *Tout idéal de $\mathbb{K}[X_1, ..., X_n]$ est engendré par un nombre fini de générateurs.*

La démonstration de ce théorème classique est par exemple faite au chapitre 2 de [7].

Par analogie avec le cas en une variable, nous allons, par la suite, voir un code correcteur comme un idéal de $\mathbb{K}[X_1, ..., X_n]/J$ où J est un idéal de $\mathbb{K}[X_1, ..., X_n]$. Cela signifie qu'il va falloir donner un sens et pouvoir manipuler le reste d'un polynôme f modulo l'idéal J.

En une variable les monômes d'un polynôme sont classés selon leur degré, en plusieurs variables il existe de nombreuses façons de bien ordonner des ensembles de monômes. Ces ordres monomiaux sont décrits et détaillés dans [7] au chapitre 2.

Exemple 5.1.4. — Pour faire des exemples de codes correcteurs multivariés tordus, nous travaillerons souvent en deux variables et l'ordre monomial utilisé sera l'ordre lexicographique avec $X > Y$, c'est-à-dire que l'on dira que $X^aY^b > X^cY^d$ si $a > c$ ou si $a = c$ et $b > d$.

Une fois un ordre monomial défini, il est possible d'effectuer la division d'un polynôme f par un idéal J. Détaillons un peu comment se passe une telle division sur un exemple :

Exemple 5.1.5. — On va utiliser l'ordre lexicographique avec $X > Y$. Soit $f = X^2Y + XY^2 + Y^2$ et $J = \langle g_1, g_2 \rangle$ où $g_1 = XY - 1$ et $g_2 = Y^2 - 1$ Comme dans le cas en une variable le but va être d'éliminer le terme de tête de f à l'aide du terme de tête de l'un des g_i. Ici les deux termes de tête des g_i divisent X^2Y, choisissons de se servir de g_1 par exemple :

$$f - Xg_1 = XY^2 + Y^2 + X.$$

Le nouveau terme de tête XY^2 est plus petit que le précédent, on poursuit la division :

$$f - Xg_1 - Yg_1 = X + Y^2 + Y.$$

Ici le monôme dominant X n'est divisible par aucun des termes de tête des g_i, on le met donc dans le reste et l'on continue :

$$(f - Xg_1 - Yg_1) - X = Y^2 + Y.$$

Ici on va utiliser g_2 puisque le terme de tête Y^2 n'est plus divisible par celui de g_1 :

$$(f - Xg_1 - Yg_1 - g_2) - X = Y + 1.$$

Au final nous avons la relation :

$$f = (X + Y)g_1 + g_2 + (X + Y + 1).$$

Le polynôme $(X + Y)g_1 + g_2$ appartient à J et $X + Y + 1$ peut être considéré comme le reste de la division de f par J.

Il apparaît cependant un problème dans cette façon de faire, il y a un choix arbitraire lorsque plusieurs termes de tête des g_i conviennent pour faire s'annuler le terme de tête de f. Si, à la première étape de notre exemple précédent, nous avions choisi g_2 nous aurions eu la relation :

$$f = (X + 1)g_2 + Xg_1 + (2X + 1).$$

Nous obtenons donc un reste différent selon nos choix de divisions.

De plus, nous avons choisi un système de générateurs de J mais il y en a bien entendu d'autres possibles, ce qui à priori peut changer également le reste obtenu.

Il apparaît alors plutôt compliqué de travailler dans le quotient $\mathbb{K}[X_1, ..., X_n]/J$.

Les bases de Gröbner servent justement à gommer ce problème. Plus précisément, une base de Gröbner d'un idéal J est un système de générateur de J tel que si l'on effectue la division d'un polynôme f par J le reste ne dépend pas de l'ordre dans lequel on va diviser. Tout ceci en ayant fixé au préalable un ordre monomial. Nous avons le théorème issu du paragraphe 2 de [7].

Théorème 5.1.6. — *Soit J un idéal de $\mathbb{K}[X_1, ..., X_n]$. Il existe $G = \{g_1, ..., g_t\}$ qui engendre l'idéal J tel que pour tout $f \in \mathbb{K}[X_1, ..., X_n]$, il existe un unique $r \in \mathbb{K}[X_1, ..., X_n]$ vérifiant les deux conditions suivantes :*

1. *Il existe $g \in J$ tel que $f = g + r$.*
2. *Aucun des monômes de r n'est divisible par un des monômes de tête des g_i.*

En particulier, avec une base de Gröbner d'un idéal nous avons la propriété agréable que le reste d'une division de f par un idéal est nul si et seulement si f appartient à l'idéal.

Il reste à justifier l'existence d'une base de Gröbner et à donner un algorithme de calcul d'une telle base.

Un travail classique sur l'idéal monomial engendré par les monômes de tête d'un idéal fait dans [7] permet de montrer la caractérisation suivante d'une base de Gröbner

Proposition 5.1.7. — *Un système de générateurs $\{g_1, ..., g_r\}$ est une base de Gröbner d'un idéal J si et seulement si le terme de tête de chaque élément de J est divisible par le terme de tête de l'un des g_i.*

Les éléments d'un base de Gröbner ont donc leur termes de tête minimaux en ce sens là.

La question que l'on se pose est comment à partir d'une base quelconque d'un idéal obtenir une base de Gröbner de cet idéal ? Nous venons de voir qu'il faut créer des polynômes de termes dominants minimaux. Pour cela on peut songer à faire s'annuler les termes de tête des g_i, la manière naturelle de le faire est d'utiliser les S-polynômes.

Définition 5.1.8. — *Soit $(f, g) \in \mathbb{K}[X_1, ..., X_n]^2$ ayant pour termes dominants respectivement $aX_1^{\alpha_1}...X_n^{\alpha_n}$ et $bX_1^{\beta_1}...X_n^{\beta_n}$. Posons $\gamma_i = \max(\alpha_i, \beta_i)$. On pose $\alpha = (\alpha_1, ..., \alpha_n)$ et de même on définit β et γ. Le S-polynôme de f et g est donné par la formule suivante :*

$$S(f, g) = \frac{1}{a} X^{\gamma-\alpha} f - \frac{1}{b} X^{\gamma-\beta} g. \tag{5.4}$$

Le point non trivial est que prendre successivement ces S-polynômes suffit à construire une base de Gröbner, ceci est également présenté dans [7].

Nous avons l'algorithme suivant pour calculer une base de Gröbner de J :

1. On part de notre idéal, J, engendré par $(g_1, ..., g_r)$. On calcule les $S(g_i, g_j)$ pour i distinct de j.
2. On calcule un des restes de $S(g_i, g_j)$ dans la division par la famille $(g_1, ..., g_r)$. Si un de ces restes, S, est non nul alors on transforme $(g_1, ..., g_r)$ en $(g_1, ..., g_r, S)$.
3. On recommence l'algorithme à l'étape 1.
4. On obtient une base de Gröbner de l'idéal J qui a les propriétés énoncées dans le théorème.

Le point crucial est que cet algorithme termine.

De plus, nous pouvons réduire une base de Gröbner obtenue par cet algorithme en enlevant les générateurs dont le terme de tête est divisible par le terme de tête d'un autre générateur et normaliser la base en prenant des générateurs unitaires.

A ordre monomial donné, tout idéal admet une unique base de Gröbner réduite.

Le principal avantage d'un base de Gröbner est de nous donner une représentation canonique de $\mathbb{K}[X_1, ..., X_n]/J$, c'est-à-dire une écriture unique modulo l'idéal.

Les bases de Gröbner dans les anneaux de Ore ont été étudiées en toute généralité par Frédéric Chyzak et Bruno Salvy dans [4] et par Müller dans [19]. Une approche concernant les bases de Gröbner dans les idéaux bilatères est faite dans [23]. Ici le cadre dans lequel on travaille est assez particulier puisque l'anneau de Ore $\mathbb{F}_q[X, \theta]$ ne comporte pas de dérivation. Une théorie simple des bases de Gröbner peut être mise en place. Elle calque la théorie classique du cas commutatif avec des adaptations mineures.

Avant tout, il convient de dire un mot sur les ordres monomiaux. En fait, sur ce point, il n'y a pas de différence entre le cas commutatif et le cas non commutatif. Un ordre monomial classique sera également un ordre monomial de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$. Dans la suite, si ce n'est pas précisé, c'est l'ordre lexicographique (avec $X_1 > ... > X_n$) qui sera utilisé. Une présentation détaillée des différents ordres monomiaux est faite dans [7] page 52.

Le but est d'arriver au résultat suivant qui est analogue au cas commutatif que l'on retrouve par exemple dans [7] page 79.

Théorème 5.1.9. — *Soit J un idéal à gauche de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$. Il existe $G = \{g_1, ..., g_t\}$ qui engendre à gauche l'idéal J tel que pour tout $f \in \mathbb{F}_q[\underline{X}^{\underline{\theta}}]$, il existe un unique $r \in \mathbb{F}_q[\underline{X}^{\underline{\theta}}]$ vérifiant les deux conditions suivantes :*

1. *Il existe $g \in J$ tel que $f = g + r$.*
2. *Aucun des monômes de r n'est divisible par un des monômes de tête des g_i.*

Il faut bien faire attention au fait que les idéaux que l'on considère sont des idéaux à gauche.

Il convient dans notre contexte particulier d'adapter un peu la définition de S-polynôme afin que les termes dominants s'annulent encore malgré l'action des automorphismes.

Définition 5.1.10. *Soit $(f, g) \in \mathbb{F}_q[\underline{X}^{\underline{\theta}}]^2$ ayant pour termes dominants respectivement $aX_1^{\alpha_1}...X_n^{\alpha_n}$ et $bX_1^{\beta_1}...X_n^{\beta_n}$. Posons $\gamma_i = \max(\alpha_i, \beta_i)$. On pose $\alpha = (\alpha_1, ..., \alpha_n)$ et de même on définit β et γ. Le S-polynôme de f et g est donné par la formule suivante :*

$$S(f, g) = \frac{1}{\theta^{\gamma-\alpha}(a)} X^{\gamma-\alpha} f - \frac{1}{\theta^{\gamma-\beta}(b)} X^{\gamma-\beta} g. \tag{5.5}$$

C'est donc bien un polynôme fabriqué pour simplifier les termes de tête de f et g.

Il est également important de remarquer que $S(f, g)$ appartient à l'idéal à gauche engendré par f et g puisque que l'on n'a effectué que des multiplications à gauche.

Mise à part cette petite adaptation nécessaire pour les polynômes tordus, le reste fonctionne exactement de la même façon que dans le cas commutatif. On obtient l'algorithme suivant qui peut être implémenté en Magma et qui permet de calculer une base de Gröbner d'un idéal à gauche.

1. On part de notre idéal à gauche, J, engendré par $(f_1, ..., f_r)$. On calcule les $S(f_i, f_j)$ pour i distinct de j.

2. On calcule un des restes de $S(f_i, f_j)$ dans la division à droite par la famille $(f_1, ..., f_r)$. Si un de ces restes, S, est non nul alors on transforme $(f_1, ..., f_r)$ en $(f_1, ..., f_r, S)$.
3. On recommence l'algorithme à l'étape 1.
4. On réduit la base de Gröbner ainsi obtenue et on la normalise comme dans le cas commutatif.
5. On obtient une base de Gröbner de l'idéal I qui a les propriétés énoncées dans le théorème.

Exemple 5.1.11. — Voyons pas à pas sur un exemple comment marche cet algorithme. Soient $\theta(x) = x^2$ et α le générateur de $\mathbb{F}_4^*$ donné par Magma. Soit J l'idéal de $\mathbb{F}_4[X^\theta, Y^\theta]$ engendré à gauche par :

$$f_1 = X^2Y + X^2 + 1,\ f_2 = X^2Y^2 + \alpha X + 1.$$

On a $S(f_1, f_2) = X^2Y + \alpha X + Y + 1$ et son reste dans la division par $\langle f_1, f_2\rangle$ qui désigne l'idéal à gauche engendré par f_1 et f_2 est non nul et vaut :

$$f_3 = X^2 + \alpha X + Y.$$

On poursuit l'algorithme en calculant $S(f_1, f_3) = X^2 + \alpha XY + Y^2 + 1$, son reste dans la division par l'idéal à gauche $\langle f_1, f_2, f_3\rangle$ vaut :

$$f_4 = \alpha^2 XY + \alpha X + Y^2 + Y + 1.$$

On a $S(f_2, f_3) = \alpha XY^2 + \alpha X + Y^3 + 1$ dont le reste est nul dans la division par $\langle f_1, f_2, f_3, f_4\rangle$ on passe à l'étape suivante.

Au final, on obtient $J = \langle f_1, f_2, f_3, f_4, \alpha^2 X + \alpha Y^3 + Y^2 + \alpha Y + \alpha, \alpha Y^5 + \alpha^2 Y^4 + \alpha^2 Y^3 + \alpha Y^2 + \alpha^2 Y, Y^4 + Y^3, \alpha Y^2 + Y, \alpha Y\rangle$. L'étape de la réduction de la base consiste à ne garder que les polynômes dont les termes de tête ne sont multiples d'aucun autre terme de tête de polynômes de la famille obtenue, il reste :

$$J = \langle \alpha^2 X + \alpha Y^3 + Y^2 + \alpha Y + \alpha, \alpha Y\rangle.$$

Enfin on normalise la base et on obtient une base de Gröbner de J qui est :

$$J = \langle X + \alpha^2 Y^3 + \alpha Y^2 + \alpha^2 Y + \alpha^2, Y\rangle.$$

Remarque 5.1.12. — Dans cet algorithme, on utilise la division d'un polynôme par une famille de polynômes. Cet algorithme se passe comme dans le cas commutatif, c'est-à-dire que l'on essaie de faire s'annuler le terme de tête du polynôme à diviser à l'aide des termes de tête des diviseurs. Lorsque qu'on ne le peut pas, on met le monôme récalcitrant dans le reste. Bien sûr cette division n'est pas unique et peut donner plusieurs restes en fonction de la manière dont on s'y prend.

Exemple 5.1.13. — Voici à présent un exemple que l'on va garder en fil rouge durant ce paragraphe pour illustrer les différentes notions que l'on va introduire. On se place dans $\mathbb{F}_4[X^\theta, Y^\theta]$ où $\theta(x) = x^2$, muni de l'ordre lexicographique. On note $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ où α est le générateur de $\mathbb{F}_4^*$ donné par Magma. Soit J l'idéal à gauche engendré par $\{f, g\}$ avec :

$$f = X^2Y^4 + X^2,\ g = X^3Y^2 + \alpha Y.$$

Une base de Gröbner minimale et réduite est donnée par les polynômes p, q et r avec :

$$p = Y^5 + Y,\ q = X^2Y^4 + X^2,\ r = X^4 + \alpha Y^3.$$

Voyons une première utilisation des bases de Gröbner dans notre contexte.

5.1.3 Degré et borne d'un idéal

Nous allons définir dans cette section le degré d'un idéal, ce degré va pouvoir se lire lorsque l'on dispose d'une base de Gröbner de notre idéal à gauche. Cette notion nous sera utile par la suite puisqu'elle déterminera directement la longueur et la dimension des codes que l'on va obtenir.

Degré d'un idéal

Définition 5.1.14. — *On appelle* ***degré*** *de l'idéal à gauche J la dimension de $\mathbb{F}_q[\underline{X}^\theta]/J$ en tant que $\mathbb{F}_q$-espace vectoriel.*

Remarque 5.1.15. —

1. Même si J n'est pas un idéal bilatère et que le quotient $\mathbb{F}_q[\underline{X}^\theta]/J$ n'a pas forcément une structure d'anneau, c'est bien un espace vectoriel sur $\mathbb{F}_q$.
2. Cette dimension peut être infinie, mais dans notre contexte pour faire des codes correcteurs, on va vouloir se placer dans le cas où la dimension est finie.

Voyons à présent un moyen rapide de voir si la dimension de $\mathbb{F}_q[\underline{X}^\theta]/J$ est finie et de la calculer.

Soit J un idéal à gauche et $(g_1, ..., g_r)$ une base de Gröbner de J. Puisque le reste dans la division par J est uniquement déterminé lorsque l'on utilise une base de Gröbner, on peut identifier l'ensemble des classes modulo J à l'ensemble des restes. Un reste a la propriété de n'avoir aucun monôme divisible par l'un des termes de tête des g_i. La dimension de $\mathbb{F}_q[\underline{X}^\theta]/J$ en tant que $\mathbb{F}_q$-espace vectoriel est égal au cardinal de

$$\{X^\alpha,\ X^\alpha \notin \langle LM(g_1), ..., LM(g_r)\rangle\}$$

où $LM(g_i)$ désigne le monôme de tête de g_i. Notons $D(J)$ cette dimension.

Proposition 5.1.16. — *Soit J un idéal et $(g_1, ..., g_t)$ une base de Gröbner de J. Alors $D(J)$ est finie si et seulement s'il existe $(i_j)_{1\leq j\leq n}$ tels que $LM(g_{i_j}) = X_j^{a_j}$ avec a_j des entiers strictement positifs.*

Démonstration. — Soit $n \geq 2$. Par l'absurde, supposons par exemple qu'il n'existe pas de g_i dont le terme dominant soit de la forme X_1^k, alors la famille de monômes $(X_1^j)_{j\geq 0}$ ne serait divisible par aucun des termes de tête des g_i. La dimension de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$ serait infinie.
Réciproquement prenons le plus petit entier a_j tel qu'il existe i avec $LM(g_i) = X_j^{a_j}$. Une famille génératrice de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$ est $\{X_1^{i_1}...X_n^{i_n}\}_{0\leq i_j\leq a_j-1}$ qui est bien de cardinal fini.

■

Exemple 5.1.17. — Si l'on reprend l'exemple 5.1.13 précédent, on a l'idéal donné par sa base de Gröbner :

$$J = \langle Y^5 + Y, X^2Y^4 + X^2, X^4 + \alpha Y^3\rangle.$$

D'après la proposition précédente, on voit immédiatement que $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$ est de dimension finie.

Celle-ci vaut 18 et une base du quotient est donnée par les monômes suivants :

$$\{Y^0, Y, ..., Y^4, XY^0, ..., XY^4, X^2Y^0, ..., X^2Y^3, X^3Y^0, ..., X^3Y^3\}.$$

C'est-à-dire l'ensemble des monômes qui ne sont pas divisibles par l'un des termes de tête des éléments de la base de Gröbner.

Un des intêrets du calcul d'une base de Gröbner est de pouvoir connaître rapidement le degré d'un idéal et pouvoir faire des opérations dans le quotient $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$ qui a maintenant une base naturelle.

Remarque 5.1.18. — Par la suite, on va chercher des idéaux à gauche de degré fini.

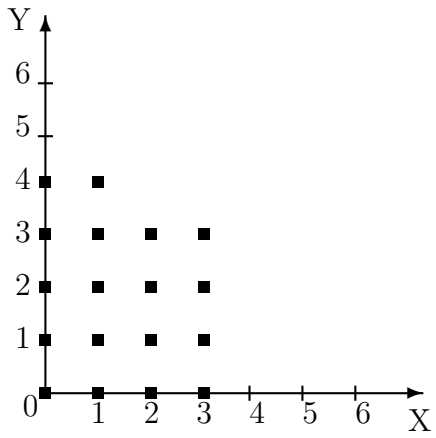
On peut remarquer tout de suite que si J est engendré à gauche par un seul élément alors le degré de J vaut 0 (cas trivial) ou est infini. Ceci dans le cas où n est différent de 1.

Vision sous forme d'escalier

Il existe une manière visuelle de représenter une base du quotient $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$.

Reprenons l'exemple précédent, on a alors l'escalier associé à l'idéal :

$$J = \langle Y^5 + Y, X^2Y^4 + X^2, X^4 + \alpha Y^3\rangle.$$



Dans ce diagramme un carré se trouve à la position (i, j) si et seulement si X^iY^j est un monôme qui n'est divisible par aucun des termes de tête de la base de Gröbner réduite de J. Ceci est équivalent à dire que le monôme en question est un élément de la base naturelle de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$.

Dans cet exemple, on visualise le fait que la dimension en tant que $\mathbb{F}_q$-espace vectoriel de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$ est finie et vaut 18.

Remarque 5.1.19. — Si $J \subset J'$ sont deux idéaux à gauche alors l'escalier de J contient l'escalier de J'. La réciproque est vraie pour des idéaux monomiaux mais fausse en général.

Existence d'une borne

Dans la construction classique des codes tordus, le polynôme générateur du code, g, doit être un diviseur à droite d'un polynôme central f. Ce qui dans le langage des idéaux se traduit par le fait que l'idéal à gauche $\langle g \rangle$ contient l'idéal bilatère $\langle f \rangle$.

Afin de généraliser cette approche, on est donc amené à étudier le problème suivant : étant donné J un idéal à gauche, existe-t-il toujours un idéal bilatère I inclus dans J tel que I soit de degré fini ? La finitude du degré étant bien sûr requise afin que la longueur du code soit finie.

Définition 5.1.20. — *Soit J un idéal à gauche de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$, on dit que I est une* ***borne*** *pour J si $I \subset J$ et I bilatère.*

Proposition 5.1.21. — *Tout idéal à gauche de degré fini possède une borne.*

Démonstration. — Soit J un idéal à gauche et $G = (f_1, ..., f_r)$ une base de Gröbner de J. Montrons que J contient un élément central. D'après la propriété sur les bases de Gröbner, pour tout $i \geq 0$, on effectue la division suivante :

$$X_1^{i|<\theta_1>|} = A_i + R_i \tag{5.6}$$

où $A_i \in J$ et R_i est le reste.
Comme le degré de J est fini par hypothèse, ces restes appartiennent à un sous-espace vectoriel sur $\mathbb{F}_q$ de dimension finie (l'espace vectoriel dont une base est formée des monômes qui ne sont pas dans l'idéal engendré par les monômes de tête des f_i). Cet espace vectoriel est de dimension finie sur $\mathbb{F}_p$ où p est la caractéristique de $\mathbb{F}_q$. Il existe donc $d \in \mathbb{N}$ et $(d_i)_{0 \leq i \leq d} \in \mathbb{F}_p$ tels que :

$$\sum_{i=0}^{d} d_i R_i = 0.$$

En effectuant la même combinaison linéaire sur les divisions écrites au-dessus, on obtient :

$$\sum_{i=0}^{d} d_i X_1^{i|<\theta_1>|} \in J.$$

On a trouvé un élément central dans J, donc $\langle \sum_{i=0}^{d} d_i X_1^{i|<\theta_1>|} \rangle \subset J$.

On pose $I = \langle \sum_{i=0}^{d} d_i X_1^{i|<\theta_1>|} \rangle$, c'est bien une borne pour J.

■

Cependant, ce qui nous intéresse est que la borne I soit également de degré fini et c'est possible :

Proposition 5.1.22. — *Tout idéal de degré fini possède une borne de degré fini.*

Démonstration. — Soit J un idéal de degré fini. Ce que l'on a fait dans la preuve précédente avec la variable X_1 dans la division 5.6, on peut le faire avec les autres variables, c'est-à-dire qu'il existe des polynômes $P_i \in \mathbb{F}_p[X_i^{|<\theta_i>|}]$ appartenant à l'idéal J. Posons $I = \langle P_1, ..., P_n \rangle$. Nous allons montrer que I est bien une borne de degré fini de J. Déjà, il est clair que I est inclus dans J et que c'est un idéal bilatère.
Remarquons ensuite que lorsque l'on effectue la division d'un élément f par l'idéal I, le reste ne contient aucun monôme divisible par l'un des termes dominants des P_i. C'est-à-dire que la dimension de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$ est au plus $\prod_{i=1}^{n} \deg_{X_i}(P_i)$.

■

Exemple 5.1.23. — Reprenons notre exemple précédent, avec J donné à l'aide d'une base de Gröbner par :

$$J = \langle Y^5 + Y, X^2Y^4 + X^2, X^4 + \alpha Y^3 \rangle.$$

En effectuant plusieurs divisions successives et en cherchant des relations linéaires, on trouve :

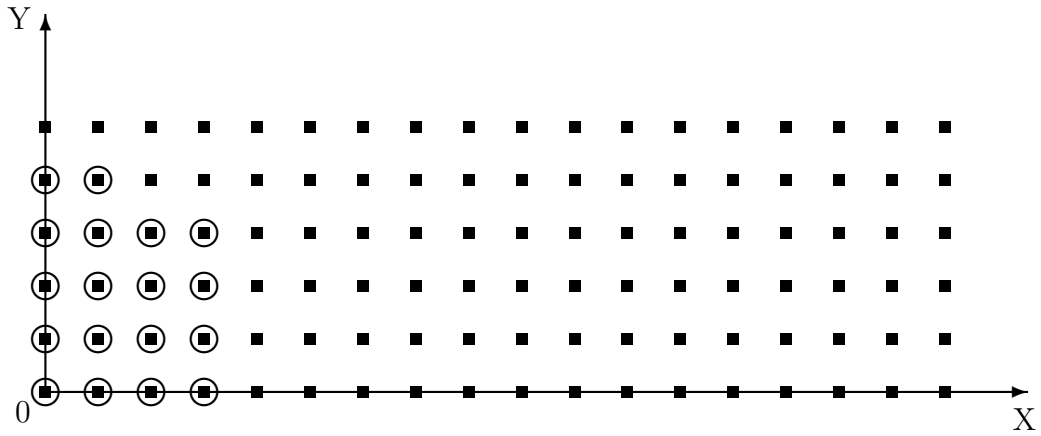
$$P_1 = X^{18} + X^2$$
$$P_2 = Y^6 + Y^2$$

qui appartiennent à J. L'idéal :

$$I = \langle X^{18} + X^2, Y^6 + Y^2 \rangle$$

est bien un idéal bilatère inclus dans J et il est de degré fini, $108 = 18 \times 6$.

Voici le graphique représentant l'escalier de J et l'escalier de I. L'escalier de I contient celui de J :



Les cercles représentent l'escalier de J et les carrés celui de I.

Borne de degré minimale

Le diagramme précédent montre que la borne I donnée par l'algorithme peut être, dans certains cas, assez grossière. On se pose naturellement la question suivante : étant donné un idéal à gauche J, peut-on trouver un idéal bilatère $I \subset J$ tel que le degré de I soit minimum ?

On voit que choisir I engendré par des polynômes à variables séparées est assez restrictif, il est fort possible qu'il y ait des polynômes mélangeant les variables qui soient super-centraux et qui appartiennent à J. En particulier l'un des défauts de la construction de l'exemple précédent est que l'escalier de I ne tient pas compte de la forme particulière de l'escalier de J.

Dans la suite le degré de la borne I va correspondre à la longueur du code correcteur, il est donc intéressant d'essayer d'optimiser ce degré.

L'algorithme suivant permet de trouver des polynômes centraux inclus dans J :

1. Soit J un idéal à gauche de degré fini, k, donné par une base de Gröbner et soit $(N_1, ..., N_n) \in \mathbb{N}^n$.
2. Pour tous les entiers $(i_1, ..., i_n) \in [0...N_1 - 1] \times ... \times [0...N_n - 1]$, on effectue la division de $X_1^{i_1|<\theta_1>|}...X_n^{i_n|<\theta_n>|}$ par l'idéal J :

$$X_1^{i_1|<\theta_1>|}...X_n^{i_n|<\theta_n>|} = A_{i_1,...,i_n} + R_{i_1,...,i_n}$$

où $A_{i_1,...,i_n} \in J$.

D'après la propriété fondamentale sur les bases de Gröbner, les restes $R_{i_1,\ldots,i_n}$ ne sont composés que de monômes non divisibles par l'un des monômes de tête des générateurs de la base de Gröbner de J. On peut convertir les $R_{i_1,\ldots,i_n}$ en des vecteurs de taille k à coefficients dans $\mathbb{F}_q$.

3. On forme la matrice en mettant en colonne les $N_1 \ldots N_n$ vecteurs ainsi obtenus et l'on voit cette matrice comme une application $\cap_{i=1}^{n}(\mathbb{F}_q)^{\theta_i}$-linéaire. On cherche une base du noyau de cette matrice. Un élement de ce noyau nous fournit une relation de dépendance linéaire entre les $R_{i_1,\ldots,i_n}$ à coefficients dans $\cap_{i=1}^{n}(\mathbb{F}_q)^{\theta_i}$. En effectuant la même relation de dépendance linéaire sur les divisions de l'étape 2, on obtient un polynôme central qui appartient à J.

   On peut faire varier les N_i et les fixer de plus en plus grands pour obtenir d'autres polynômes centraux.

4. On forme l'idéal bilatère I engendré par les polynômes centraux ainsi trouvés.

Remarque 5.1.24. — Si l'on prend $N_i \geq \frac{deg(P_i)}{|<\theta_i>|}$ alors les polynômes P_i de la proposition 5.1.22 vont être pris en compte par l'algorithme précédent, ainsi on sera assuré que l'idéal I trouvé est bien de degré fini.

Définition 5.1.25. — *Soit J un idéal à gauche de degré fini. On appelle* ***idéal bilatère maximal*** *associé à J et on note J^* l'idéal engendré par l'ensemble des polynômes centraux appartenant à J.*

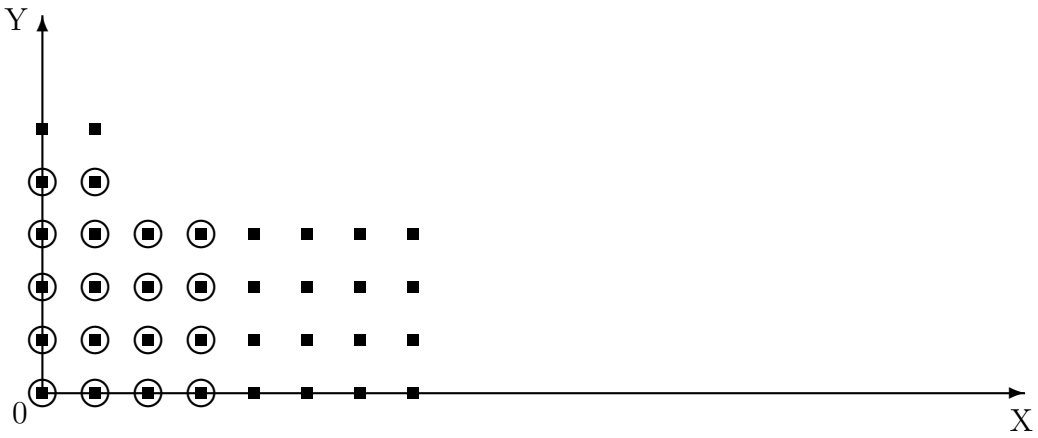
On va, dans les exemples que l'on va considérer par la suite, prendre les N_i suffisamment grands afin d'avoir une borne, I, assez proche de J sans forcément être l'idéal bilatère maximal associé à J.

Exemple 5.1.26. — Revenons à notre exemple précédent, c'est-à-dire $J = \langle Y^5+Y, X^2Y^4+X^2, X^4+\alpha Y^3\rangle$, on avait trouvé une borne pour J de degré 108, en fait il est possible de faire mieux en utilisant l'algorithme décrit précédemment.

Avec $N_1 = N_2 = 10$, on trouve un certain nombre de polynômes centraux inclus dans J et une base de Gröbner de l'idéal engendré par les polynômes centraux ainsi obtenus est :

$$I = \langle Y^6 + Y^2, X^2Y^4 + X^2, X^8 + Y^2\rangle.$$

Le degré de I est 36, de plus si l'on dessine les escaliers correspondants aux idéaux I et J, on voit que la forme de I est moins grossière et mieux adaptée à l'idéal J que précédemment.



5.1.4 Bases de Gröbner pour les idéaux bilatères

Afin de travailler avec l'idéal I on est amené à calculer une base de Gröbner d'un idéal engendré par des polynômes centraux. Remarquons tout de suite la propriété suivante :

Proposition 5.1.27. *Soit $I = \langle f_1, ...f_r\langle$ un idéal où les f_i sont super-centraux et soit $I = \langle g_1, ..., g_t\rangle$ une base de Gröbner de I, alors les g_i sont super-centraux.*

Démonstration. — Pour montrer cela remarquons deux choses :

1. Le S-polynôme de deux polynômes super-centraux est super-central d'après la formule 5.5.
2. Lorsque l'on effectue l'algorithme de division d'un polynôme super-central par d'autre polynômes super-centraux, le reste est un polynôme super-central. En effet tout se passe comme si l'on travaillait dans l'anneau $(\cap_{i=1}^{n}(\mathbb{F}_q)^{\theta_i})[X_1^{|<\theta_1>|}, ..., X_n^{|<\theta_n>|}]$.

■

Nous avons à présent tous les outils pour voir comment fabriquer un code correcteur à l'aide de ces anneaux de Ore multivariés.

5.2 Obtention de codes multivariés

5.2.1 Propriétés sur les mots du code

Soit J un idéal à gauche de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$ de degré fini et I une borne de J de degré fini n. Après avoir pris une base de Gröbner pour I, il existe une base naturelle du quotient $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$ qui est de cardinal n. Par le théorème de correspondance des idéaux, J peut être vu comme un idéal à gauche de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$ puisqu'il contient I. A chaque polynôme de

l'idéal, on associe alors un mot de $\mathbb{F}_q^n$ dont les composantes sont juste les coordonnées du polynôme dans la base de $\mathbb{F}_q[\underline{X^\theta}]/I$.

Il y a ainsi une application qui à un idéal de $\mathbb{F}_q[\underline{X^\theta}]/I$ associe un code sur $\mathbb{F}_q$. C'est une généralisation naturelle de la construction des θ-codes. Néanmoins si l'on traduit en terme de mots du code la stabilité par multiplication à gauche par X_i, on obtient des propriétés bien particulières du code.

Voyons à quoi ressemblent ces propriétés que l'on a sur les mots dans un exemple simple.

Exemple 5.2.1. — Prenons un exemple simplifié : le cas des codes multi-θ-cycliques.

Soit J un idéal à gauche de $\mathbb{F}_q[X^{\theta_1}, Y^{\theta_2}]/\langle X^r - 1, Y^s - 1\rangle$.

Si $P \in J$ avec :

$$P = a_{0,0} + a_{0,1}Y + ... + a_{0,s-1}Y^{s-1} + a_{1,0}X... + a_{r-1,s-1}X^{r-1}Y^{s-1}$$

alors

$$XP = \theta(a_{0,0})X + \theta(a_{0,1})XY + ... + \theta(a_{0,s-1})XY^{s-1} + \theta(a_{1,0})X^2... + \theta(a_{r-1,s-1})Y^{s-1}.$$

Donc finalement la stabilité par multiplication par X se traduit par la condition suivante sur les mots du code C :

$$(a_{0,0}, a_{0,1}, ...a_{0,s-1}, a_{1,0}, a_{1,1}, ..., a_{1,s-1}, ...a_{r-1,0}, a_{r-1,1}, ...a_{r-1,s-1}) \in \mathcal{C}$$

$$\Longleftrightarrow$$

$$(\theta(a_{r-1,0}), ..., \theta(a_{r-1,s-1}), \theta(a_{0,0}), ...\theta(a_{0,s-1}), ..., \theta(a_{r-2,0}), ..., \theta(a_{r-2,s-1})) \in \mathcal{C}.$$

En fait c'est comme si le code était cyclique par blocs.

Si l'on traduit à présent la condition de stabilité par multiplication par Y, on obtient la condition suivante sur les mots :

$$(a_{0,0}, a_{0,1}, ...a_{0,s-1}, a_{1,0}, a_{1,1}, ..., a_{1,s-1}, ...a_{r-1,0}, a_{r-1,1}, ...a_{r-1,s-1}) \in \mathcal{C}$$

$$\Longleftrightarrow$$

$$(\theta(a_{0,s-1}), ..., \theta(a_{0,s-2}), \theta(a_{1,s-1}), ..., \theta(a_{1,s-2}), ...\theta(a_{r-1,s-1}), ...\theta(a_{r-1,s-2})) \in \mathcal{C}.$$

C'est-à-dire qu'à l'intérieur de chacun des r blocs de taille s, il y a un décalage circulaire.

Ici c'est un cas assez simple où les polynômes de l'idéal ont une forme agréable. Dans le cas général, même s'il y a des décalages circulaires sur les blocs et à l'intérieur des blocs, ces décalages sont perburbés par l'apparition de nouveaux termes comme dans le cas des θ-codes qui ne sont pas θ-cycliques.

5.2.2 Algorithme utilisé

Voici les étapes de l'algorithme mis en oeuvre pour obtenir les exemples de codes qui vont suivre.

1. On se place dans $\mathbb{F}_q[\underline{X^\theta}]$ (qui sera souvent $\mathbb{F}_4[X^\theta, Y^\theta]$). On choisit un idéal à gauche J. En pratique, on prendra souvent J engendré par deux polynômes.
2. On calcule la base de Gröbner réduite de J. Grâce à cette base de Gröbner, on peut connaître le degré de J. Si $0 < \deg(J) < +\infty$ on continue, sinon on choisit un autre idéal.
3. On calcule une borne pour J, que l'on note I à l'aide de l'algorithme présenté dans le chapitre précédent.
4. On voit les éléments de $J \subset \mathbb{F}_q[\underline{X^\theta}]/I$ comme des $\deg(I)$-uplets qui forment les mots d'un code.

Nous allons voir un moyen simple de prévoir les paramètres du code ainsi obtenu et surtout d'avoir facilement la matrice génératrice sous forme systématique du code.

5.3 Dimension du code et matrice génératrice

Le but de ce paragraphe est de montrer que l'on peut prévoir la dimension du code que l'on obtient ainsi que la matrice génératrice sous forme systématique.

5.3.1 Cadre et notations

Soit J un idéal à gauche de degré k, c'est-à-dire qu'une base de l'espace vectoriel sur $\mathbb{F}_q$, $\mathbb{F}_q[\underline{X^\theta}]/J$, a pour cardinal k. Notons cette base $E = \{e_1, ..., e_k\}$. On remarque que les éléments de cette base sont des monômes, plus précisément ce sont les monômes qui ne sont pas divisibles par l'un des monômes de tête d'un élément de J ou de manière équivalente par l'un des monômes de tête des éléments d'une base de Gröbner de J.

Soit $I \subset J$ une borne pour J avec $\deg(I) = n$. Notons une base de $\mathbb{F}_q[\underline{X^\theta}]/I$ en tant que $\mathbb{F}_q$-espace vectoriel $F = \{e_1, ..., e_k, f_1, .., f_{n-k}\}$. On peut choisir une base de cette forme là comme $I \subset J$ (en effet les monômes qui ne sont divisibles par aucun des termes de tête des éléments de J ne sont, a fortiori, divisibles par aucun des termes de tête des éléments de I). On note $\mathcal{C}$ le code correcteur ainsi obtenu.

5.3.2 Résultat

On a la proposition suivante sur la dimension du code $\mathcal{C}$.

Proposition 5.3.1. *La dimension de $\mathcal{C}$ est $n - k$.*

Remarque 5.3.2. — Comme attendu cela correspond à ce qui se passe pour les codes tordus en une variable. En effet, si g est le polynôme générateur du code de degré k et f une borne de degré n, on sait que le code a pour dimension $n - k$.

Démonstration. — Le code $\mathcal{C}$ est formé de l'ensemble des restes des éléments de J dans la division par I.
Montrons pour commencer que $dim(\mathcal{C}) \geq n-k$.
En conservant les notations du préambule, effectuons la division de f_i par l'idéal J :

$$f_i = R_i - \sum_{j=1}^{k} \beta_i^j e_j$$

où $R_i \in J$ donc

$$R_i = f_i + \sum_{j=1}^{k} \beta_i^j e_j$$

est un élément de J. Regardons à quel mot du code il correspond, c'est-à-dire quel est son reste dans la division par I. On a :

$$R_i = 0 + R_i$$

en effet les monômes de R_i font partie de la base F.
En écrivant les coordonnées dans la base F, on a le mot suivant qui appartient à $\mathcal{C}$:

$$(\beta_i^1, ..., \beta_i^k, \delta_i^1, ..., \delta_i^{n-k})$$

où δ est le symbole de Kronecker.
La dimension de $\mathcal{C}$ est donc au moins $n-k$.
La base de F n'est peut être pas rangée par ordre lexicographique mais une permutation de la base ne change pas le résultat sur la dimension du code.
Montrons à présent que la dimension du code est exactement $n-k$.
Pour cela montrons que $Vect\{e_1, ..., e_k\} \cap C = \{0\}$ et cela nous permettra de conclure d'après la formule des dimensions de Grassman.
Soit m appartenant à l'intersection, il existe donc $P \in J$ tel que :

$$P = R + m$$

où $R \in I$.
Donc $m = P - R$ est dans J. C'est absurde au vu des monômes qui composent m sauf si $m = 0$.
D'où le résultat.

■

Remarque 5.3.3. Grâce à la forme du mot de code correspondant à R_i, on remarque que la distance minimale de $\mathcal{C}$ vérifie :

$$d(\mathcal{C}) \leq k + 1. \tag{5.7}$$

Ce qui correspond à la borne de Singleton.

La méthode précédente va nous permettre de former une matrice génératrice et une matrice de parité du code.

5.3.3 Matrice génératrice

Dans la démonstration du chapitre précédent, il ressort que les mots :

$$c_i = (\beta_i^1, \beta_i^2, ..., \beta_i^k, \delta_i^1, ..., \delta_i^{n-k})$$

forment une base du code. Si l'on change l'ordre de la base en $(f_1, ..., f_{n-k}, e_1, ..., e_k)$ et que l'on met chacun des mots de la base du code en ligne, on obtient la matrice génératrice suivante de taille $(n-k) \times n$:

$$\left(\begin{array}{c|c} Id_{n-k} & (\beta_i^j) \end{array} \right).$$

On remarque que cette matrice génératrice est la matrice génératrice sous forme générique.

5.3.4 Matrice de parité

Ayant la matrice génératrice sous forme générique, on peut facilement en déduire la matrice de parité, celle-ci est de taille $(n-k) \times n$ et s'écrit :

$$\left(\begin{array}{c|c} -\beta_j^i & Id_{n-k} \end{array} \right).$$

5.4 Exemples et tableaux de résultats

5.4.1 Quelques exemples

Voyons à présent quelques exemples de codes correcteurs que l'on obtient. On suit la construction présentée dans l'algorithme 5.2.2.

Exemple 5.4.1. —

1. On se place dans $\mathbb{F}_4[X^\theta, Y^\theta]$ où $\theta(x) = x^2$.
2. Soient
$$P = \alpha X^2 + \alpha XY^2 + XY + X + \alpha^2 Y^2 + Y + \alpha^2$$
$$Q = \alpha X^2 Y^2 + X^2 Y + \alpha X^2 + XY^2 + X + Y^2 + Y + 1.$$
On note $J = \langle P, Q \rangle$ l'idéal à gauche engendré par P et Q.
3. Une base de Gröbner à gauche engendrée par P et Q est engendrée à gauche par les polynômes suivants :
$$P' = X^2 + XY^2 + \alpha^2 XY + \alpha^2 X + \alpha Y^2 + \alpha^2 Y + \alpha$$
$$Q' = XY + \alpha^2 X + \alpha Y^4 + Y^3 + Y^2 + \alpha^2 Y$$
$$R' = Y^3 + \alpha Y^2 + \alpha^2 Y + 1.$$
L'idéal J est de degré 4 et une base du $\mathbb{F}_4$-espace vectoriel $\mathbb{F}_4[X^\theta, Y^\theta]/J$ est $\{1, Y, Y^2, X\}$.

4. Si l'on prend $N_1 = N_2 = 10$, on obtient l'idéal I donné avec sa base de Gröbner :

$$I = \langle X^2 + 1, Y^6 + 1 \rangle.$$

On remarque d'ailleurs que ces polynômes ne sont autres que P_1 et P_2 définis dans la preuve de la proposition 5.1.22.

5. En effectuant les quelques divisions décrites au chapitre précédent, on obtient un code de paramètres $[12, 8, 4]$ sur $\mathbb{F}_4$ qui a pour matrice génératrice sous forme systématique :

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha^2 & \alpha & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & \alpha^2 & \alpha^2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & \alpha^2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha & \alpha^2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \alpha^2 & 0 & \alpha^2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \alpha & \alpha & 1 & \alpha^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & \alpha & \alpha & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha^2 & \alpha & 0 & \alpha^2 \end{pmatrix}.$$

Exemple 5.4.2. —

1. Prenons cette fois l'anneau $\mathbb{F}_9[X^\theta, Y^\theta]$ où $\theta(x) = x^3$ muni de l'ordre lexicographique classique. On note α le générateur de $\mathbb{F}_9^*$ donné par Magma.

2. Soit $J = \langle f, g \rangle$ l'idéal à gauche engendré par :

$$f = X^2Y^2 + \alpha^7X^2Y + \alpha^2X^2 + XY^2 + \alpha XY + \alpha^6X + \alpha^2Y^2 + \alpha^5Y + \alpha^6$$

$$g = \alpha^6X^2Y^2 + \alpha^3X^2Y + \alpha X^2 + 2XY^2 + \alpha^3XY + X + \alpha^6Y^2 + \alpha Y + \alpha^6.$$

3. Une base de Gröbner de J est donnée par :

$$p = X + \alpha^5Y^5 + \alpha Y^4 + Y^3 + Y^2 + \alpha^2$$

$$q = Y^3 + Y^2 + \alpha^2Y + \alpha^2.$$

On remarque que J est bien de degré fini.

4. Une borne de degré fini de J est :

$$I = \langle X^2 + \alpha^3, Y^6 + \alpha^3Y^4 + \alpha^6Y^2 + \alpha^3 \rangle.$$

5. On obtient alors un code de paramètres $[12, 9, 3]$ sur $\mathbb{F}_9$.

5.4.2 Résultats

Les tableaux suivant résument les codes obtenus en choisissant aléatoirement deux polynômes f et g de degré 2 à coefficients dans $\mathbb{F}_4$ et en appliquant l'algorithme 5.2.2 à l'idéal $J = \langle f, g \rangle$. En pratique dans la plupart des cas, l'idéal J est trivial. Lorsque ce n'est pas le cas le tableau suivant présente les codes obtenus. Ils sont classés en colonne par leur distance minimale et en ligne par leur longueur.

Minimale distance	2	3	4	5	6
$n = 4$	$[4, 1, 4]$ $[4, 1, 2]$ $[4, 2, 2]$				
$n = 8$	$[8, 5, 2]$ $[8, 6, 2]$ $[8, 4, 2]$ $[8, 3, 2]$	$[8, 4, 3]$ $[8, 5, 3]$	$[8, 4, 4]$		
$n = 12$	$[12, 10, 2]$ $[12, 9, 2]$ $[12, 8, 2]$ $[12, 7, 2]$ $[12, 6, 2]$	$[12, 9, 3]$ $[12, 7, 3]$ $[12, 8, 3]$ $[12, 6, 3]$	$[12, 8, 4]$ $[12, 7, 4]$ $[12, 6, 4]$	$[12, 6, 5]$	
$n = 16$	$[16, 12, 2]$ $[16, 11, 2]$ $[16, 13, 2]$ $[16, 10, 2]$ $[16, 9, 2]$	$[16, 12, 3]$ $[16, 10, 3]$ $[16, 11, 3]$	$[16, 11, 4]$ $[16, 10, 4]$		$[16, 8, 6]$
$n = 20$	$[20, 13, 2]$ $[20, 15, 2]$ $[20, 17, 2]$ $[20, 14, 2]$ $[20, 16, 2]$ $[20, 12, 2]$	$[20, 15, 3]$ $[20, 14, 3]$ $[20, 13, 3]$ $[20, 12, 3]$	$[20, 15, 4]$ $[20, 14, 4]$ $[20, 13, 4]$ $[20, 12, 4]$		
$n = 24$	$[24, 20, 2]$ $[24, 18, 2]$ $[24, 17, 2]$ $[24, 21, 2]$ $[24, 19, 2]$ $[24, 16, 2]$	$[24, 18, 3]$ $[24, 17, 3]$ $[24, 19, 3]$ $[24, 16, 3]$	$[24, 17, 4]$ $[24, 18, 4]$ $[24, 16, 4]$		
$n = 28$	$[28, 23, 2]$ $[28, 21, 2]$ $[28, 20, 2]$ $[28, 22, 2]$	$[28, 21, 3]$ $[28, 20, 3]$ $[28, 22, 3]$	$[28, 21, 4]$ $[28, 20, 4]$		

On remarque que la dimension du code est assez proche de la longueur du code, c'est-à-dire que $D(J) = k$ est petit devant $D(I) = n$. En effet, dans la plupart des cas, même

si J est de degré à priori petit car engendré par des polynômes de degré 2, le degré de la borne explose souvent.

Voilà quelques résultats pour des polynômes de degré 3.

Distance minimale	2	3	4
$n = 4$	$[4, 2, 2]$ $[4, 1, 2]$		
$n = 8$	$[8, 6, 2]$ $[8, 5, 2]$ $[8, 4, 2]$	$[8, 5, 3]$ $[8, 4, 3]$	$[8, 4, 4]$
$n = 12$	$[12, 10, 2]$ $[12, 8, 2]$ $[12, 6, 2]$ $[12, 9, 2]$ $[12, 7, 2]$	$[12, 8, 3]$ $[12, 9, 3]$ $[12, 7, 3]$	$[12, 7, 4]$
$n = 16$	$[16, 12, 2]$ $[16, 11, 2]$ $[16, 13, 2]$ $[16, 10, 2]$	$[16, 12, 3]$ $[16, 11, 3]$	$[16, 10, 4]$ $[16, 11, 4]$
$n = 20$	$[20, 15, 2]$ $[20, 16, 2]$ $[20, 14, 2]$ $[20, 13, 2]$ $[20, 17, 2]$	$[20, 15, 3]$ $[20, 14, 3]$	$[20, 14, 4, 6]$
$n = 24$	$[24, 18, 2]$ $[24, 18, 3]$ $[24, 19, 2]$ $[24, 17, 2]$ $[24, 21, 2]$ $[24, 20, 2]$	$[24, 17, 3]$ $[24, 19, 3]$	$[24, 18, 4]$ $[24, 16, 4]$ $[24, 17, 4]$
$n = 28$	$[28, 21, 2]$ $[28, 22, 2]$ $[28, 20, 2]$ $[28, 23, 2]$	$[28, 21, 3]$ $[28, 18, 3]$ $[28, 20, 3]$	$[28, 21, 4]$ $[28, 20, 4]$
$n = 32$	$[32, 24, 2]$ $[32, 25, 2]$ $[32, 27, 2]$ $[32, 26, 2]$ $[32, 23, 2]$ $[32, 28, 2]$	$[32, 24, 3]$	$[32, 24, 4]$ $[32, 23, 4]$
$n = 36$	$[36, 27, 2]$ $[36, 29, 2]$ $[36, 25, 2]$ $[36, 26, 2]$	$[36, 27, 3]$ $[36, 28, 3]$	$[36, 27, 4]$ $[36, 26, 4]$
$n = 40$	$[40, 35, 2]$ $[40, 33, 2]$ $[40, 32, 2]$		$[40, 30, 4]$
$n > 40$	$[48, 43, 2]$ $[48, 44, 2]$ $[48, 42, 2]$ $[52, 41, 2]$ $[88, 82, 2]$	$[48, 41, 3]$	$[44, 33, 4]$ $[76, 64, 4]$

5.5 Codes modules multivariés

Le chapitre 4 a mis en lumière le fait que l'on peut s'affranchir de chercher des idéaux bilatères, I, si l'on ne tient pas à tout prix à ce que $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$ ait une structure d'anneau. Cela permet d'étendre encore la famille de codes que l'on étudie.

Dès lors, nous n'avons plus besoin de déterminer un idéal bilatère inclus dans J mais uniquement un idéal I quelconque inclus dans J. Cela peut se faire simplement en regardant l'idéal à gauche engendré par certains éléments de J. La méthode d'obtention de la matrice génératrice se fait exactement de la même manière.

Il est intéressant de pouvoir contrôler la longueur du code que l'on veut obtenir, cette longueur correspond au degré de l'idéal $I \subset J$. Plus précisément, nous aimerions contrôler la forme de l'escalier correspondant à l'idéal I, cet escalier doit être un sur-escalier de J.

Notation 8. — Soit J un idéal de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$, on note $\Gamma(J)$ l'escalier correspondant à l'idéal J, la représentation graphique d'un tel objet est définie au paragraphe 5.1.3.

Définition 5.5.1. *Soit J un idéal de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$. On appelle* ***escalier couvrant*** *de J un escalier qui contient $\Gamma(J)$.*

La question naturelle que l'on se pose est la suivante : étant donné un escalier couvrant de J, $\mathcal{E}$, existe t'-il un idéal $I \subset J$ tel que $\Gamma(I) = \mathcal{E}$?

Remarque 5.5.2. — Dans le cas à une variable cette question se résume à : étant donné un polynôme g de degré k, a-t-il un multiple f de degré n ? Cette assertion est bien sûr vraie pour chaque $n \geq k$. Pour les codes modules à une variable, c'est juste le polynôme générateur g et la longueur du code n qui permettent d'obtenir la matrice génératrice du code, la forme explicite du multiple de g, f n'ayant pas d'importance. Dans le contexte multivarié, c'est également le cas, si l'on regarde attentivement la méthode d'obtention de la matrice génératrice présentée dans le paragraphe 5.3, il nous suffit de connaître la base canonique de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$ et l'idéal J sous forme de base de Gröbner.

Voyons à présent un exemple pour mieux appréhender ces phénomènes.

Voici un exemple de la variation des paramètres d'un code en fonction de l'escalier couvrant choisi. On se place dans $\mathbb{F}_4[X^\theta, Y^\theta]$ où θ est l'automorphisme de Frobenius. On va travailler avec les polynômes suivants :

$$P = X^2Y + \alpha X^2 + \alpha^2 XY^3 + XY^2 + \alpha X + \alpha Y^2 + Y$$

$$Q = \alpha X^2Y^2 + \alpha XY^3 + XY^2 + \alpha^2 XY + \alpha Y^2 + Y + \alpha.$$

La base de Gröbner normalisée, réduite est donnée par les polynômes suivants :

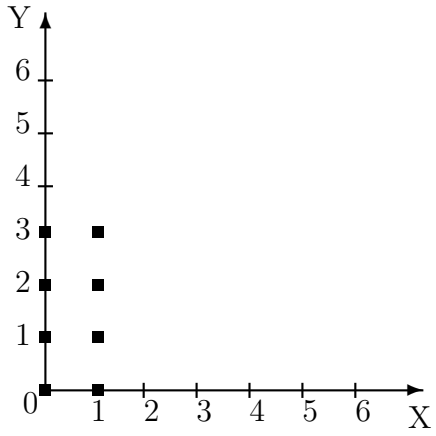
$$P' = X^2 + \alpha XY^4 + \alpha XY^3 + XY + X + \alpha^2 Y^3 + Y^2 + 1$$

$$Q' = Y^4 + 1.$$

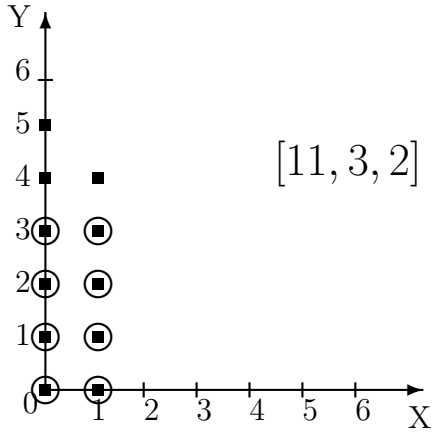
Le degré de cet idéal, J, est 8, une base de $\mathbb{F}_q[X^\theta, Y^\theta]/J$ est donnée par les monômes suivants :

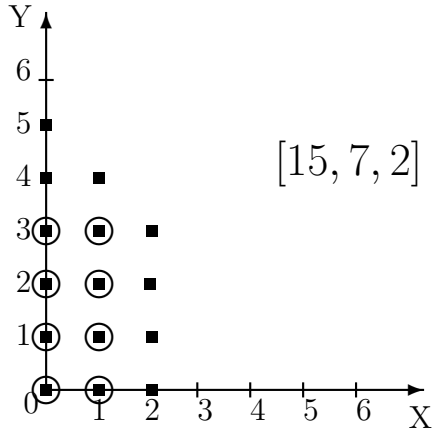
$$\{1, Y, Y^2; Y^3, X, XY, XY^2, XY^3\}.$$

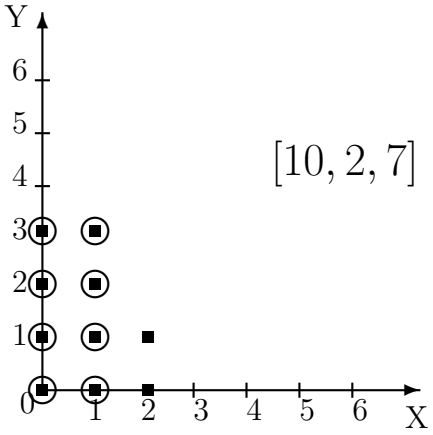
L'escalier correspondant a la forme rectangulaire suivante

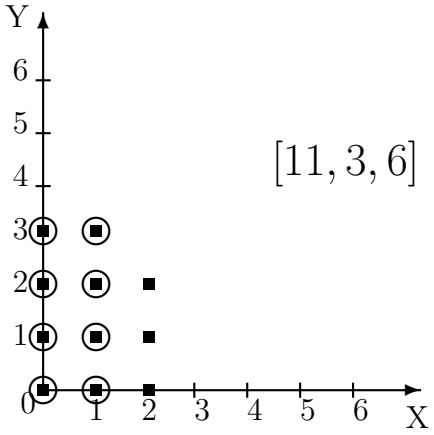


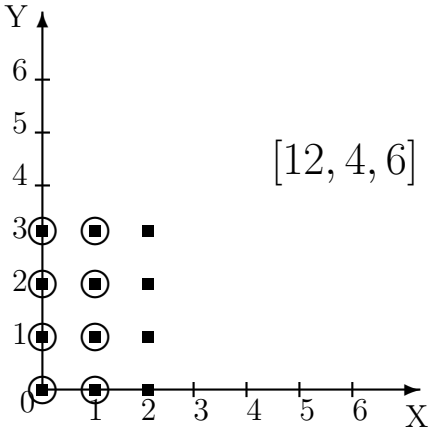
Nous allons à présent prendre plusieurs sur-escaliers et regarder les codes qui en découlent.

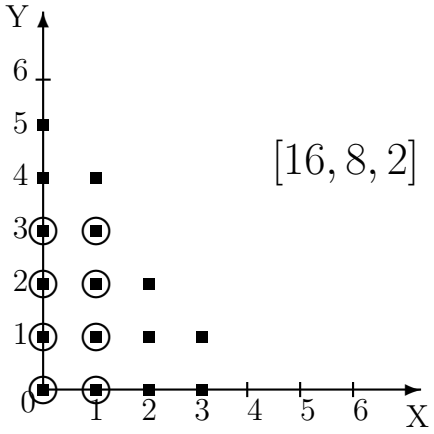


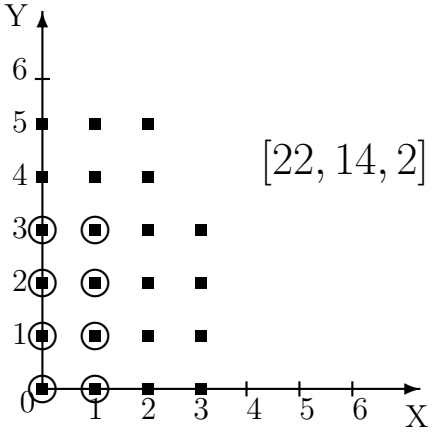


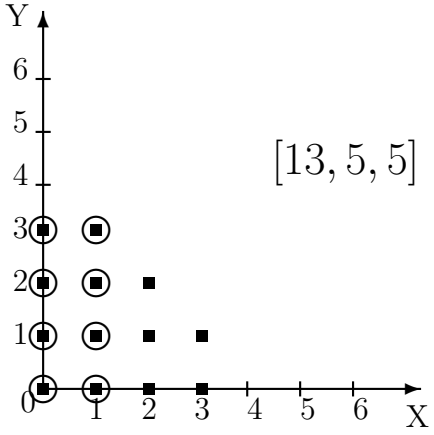

Y
X
0 1 2 3 4 5 6
[10, 2, 7]

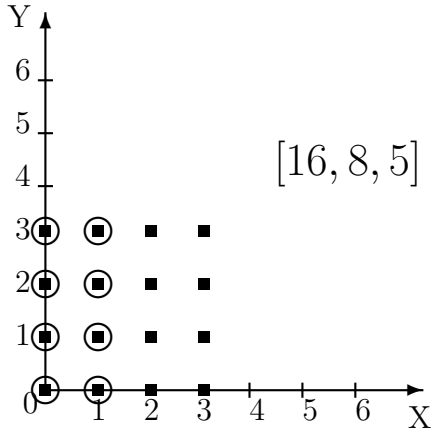

Y
X
0 1 2 3 4 5 6
[11, 3, 6]

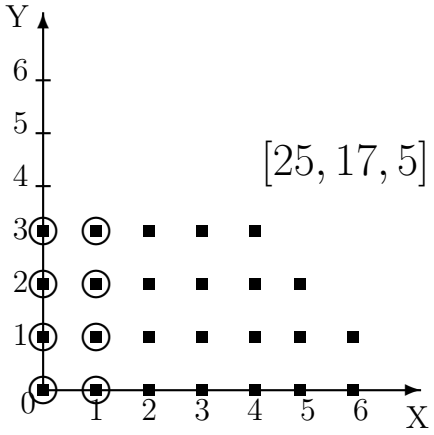

Y
X
0 1 2 3 4 5 6
[12, 4, 6]

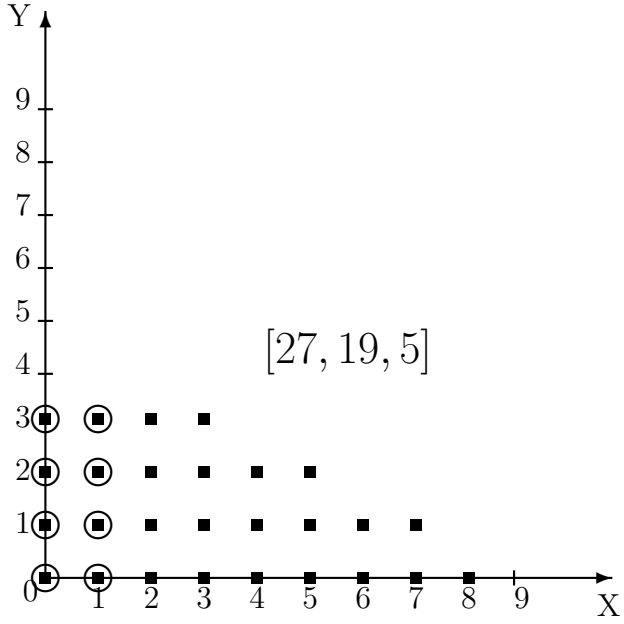

Y
X
0 1 2 3 4 5 6
[16, 8, 2]

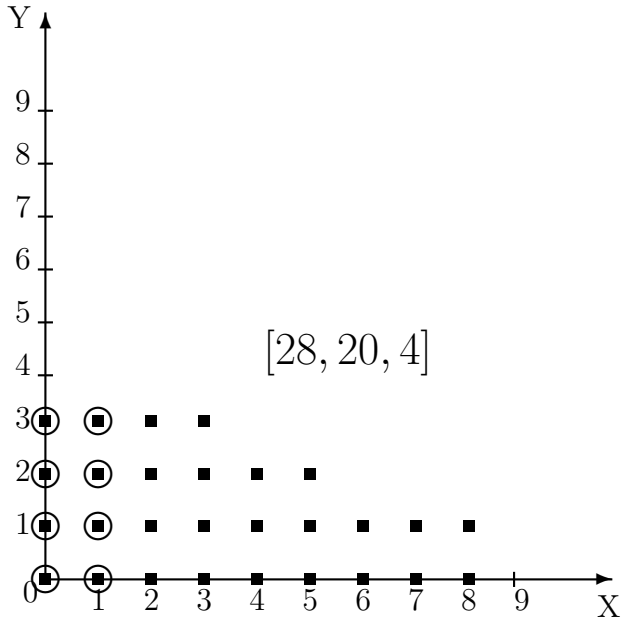

Y
X
0 1 2 3 4 5 6
[22, 14, 2]

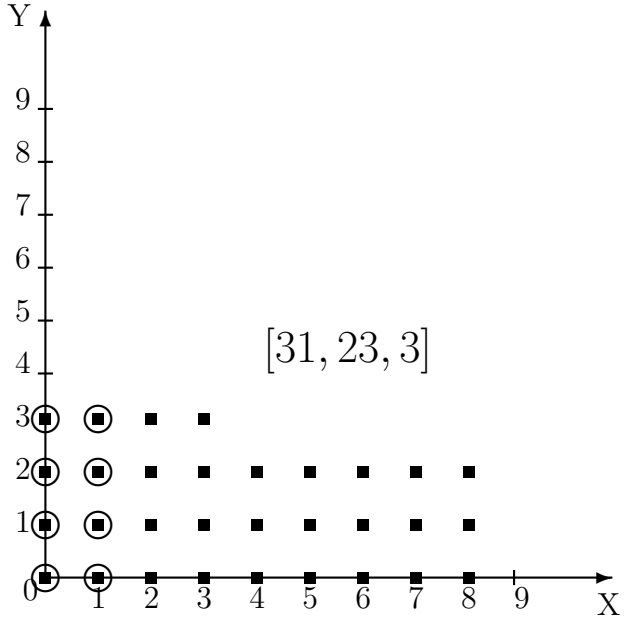

Y
X
0 1 2 3 4 5 6
[13, 5, 5]


Y
6
5
4
3
2
1
0
1
2
3
4
5
6
X
[16, 8, 5]


Y
6
5
4
3
2
1
0
1
2
3
4
5
6
X
[25, 17, 5]


Y
9
8
7
6
5
4
3
2
1
0
1
2
3
4
5
6
7
8
9
X
[27, 19, 5]





Il y a plusieurs choses que l'on peut remarquer sur cet exemple.

Si on a $E \subset E'$ deux sur-escaliers alors le code correspondant à E a une distance minimale supérieure ou égale au code correspondant à E'. Ceci est immédiat avec la méthode de construction de la matrice génératrice présentée au paragraphe 5.3.

Il n'y a aucune certitude sur le fait que l'escalier couvrant considéré corresponde bien à un idéal I contenu dans J néanmoins cette méthode permet de construire une famille de codes correcteurs dont on peut contrôler la dimension à partir d'un idéal à gauche d'un

anneau de polynômes multivarié.

Chapitre 6

Perspectives

6.1 Etude de la famille des codes modules

Nous allons donner quelques éléments d'étude d'un problème de stabilité des codes modules sous l'effet de diverses applications linéaires.

Si l'on fixe $\mathbb{F}_q$ un corps fini et θ un automorphisme de $\mathbb{F}_q$, on note $C_{n,r}$ l'ensemble des codes modules engendrés par un polynôme de degré r et de longueur n. Chacun des éléments de cet ensemble a une matrice génératrice de la forme :

$$G = \begin{pmatrix} g_0 & \dots & g_{r-1} & g_r & 0 & \dots & 0 \\ 0 & \theta(g_0) & \dots & \theta(g_{r-1}) & \theta(g_r) & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \dots & 0 & \theta^{n-r-1}(g_0) & \dots & \theta^{n-r-1}(g_{r-1}) & \theta^{n-r-1}(g_r) \end{pmatrix}.$$

où le polynôme générateur du code est $g(X) = g_0 + g_1X + ... + g_rX^r$.

Il peut être intéressant de se demander :

1. Quelles applications de $\mathbb{F}_q^n$ préservent $C_{n,r}$?
2. Quelles applications laissent fixe un code module donné ?

Outre l'intérêt théorique de ces questions, une connaissance du comportement de $C_{n,r}$ sous l'action de permutations par exemple, peut avoir des applications dans le **cryptosystème de McEliece**. C'est un protocole cryptographique utilisant une famille de codes correcteurs dont la sécurité repose en particulier sur l'indistinguabilité d'un code permuté de cette famille d'un code linéaire quelconque. Pour une explication de ce cryptosystème, on pourra consulter l'article fondateur de McEliece [17].

En ce qui concerne les applications laissant fixe un code, nous allons principalement nous intéresser aux applications linéaires qui préservent également le poids d'un mot, c'est-à-dire des applications ϕ telles que pour tout code, $\mathcal{C}$ de $\mathbb{F}_q^n$:

$$d(\phi(\mathcal{C})) = d(\mathcal{C}).$$

Ces applications sont exactement les **applications monomiales**, une étude très complète est faite dans le livre [2].

Notation 9. — Nous noterons $Aut(\mathcal{C})$ l'ensemble des applications monomiales préservant le code $\mathcal{C}$.

Il est, en général, difficile d'exhiber l'ensemble des automorphismes d'un code quelconque. Cela peut néanmoins être étudié pour des familles de codes particulières, par exemple Thierry Berger dans [1] a obtenu des résultats sur l'ensemble des automorphismes d'un code de Gabidulin pour la métrique rang.

6.1.1 Reconnaissance d'un code module

Avant de mener une telle étude, il faut au préalable pouvoir reconnaître un code module qui n'est pas forcément donné par sa matrice génératrice sous forme usuelle.

Nous allons voir un algorithme qui va permettre de déterminer rapidement si une matrice est la matrice génératrice d'un code module et de trouver le cas échéant le polynôme générateur.

Soit $\mathcal{C}$ le code module engendré par $g(X) = g_0+g_1X+...g_rX^r$ et G la matrice génératrice qui en découle. On considère $\hat{G}$ une autre matrice génératrice de $\mathcal{C}$, c'est-à-dire une matrice dont les lignes forment également une base du code.

Notons $q_1, ..., q_{n-r}$ les polynômes de $\mathbb{F}_q[X, \theta]$ correspondant aux lignes de $\hat{G}$, ce sont des multiples à gauche de g puisque tous les mots du code sont issus de multiples à gauche de g.

Proposition 6.1.1. — *Le plus grand diviseur commun à droite de la famille* $\{q_1, ..., q_{n-r}\}$ *est le polynôme générateur du code* g.

Démonstration. — Déjà nous venons de voir que g est un diviseur commun à droite à tous les q_i. Montrons que c'est le plus grand.
Par l'absurde notons h le pgcd à droite des $q_1, ..., q_{n-r}$ et supposons que $\deg(h) > \deg(g)$. Nous avons les relations suivantes :

$$q_j = t_j h.$$

Le polynôme h est de degré strictement supérieur à r donc comme les q_j sont de degré au plus $n-1$ on a $\deg(t_j) \leq n-r-2$. Il existe donc une combinaison linéaire :

$$\sum_{j=1}^{n-r} t_j = 0.$$

En répercutant la combinaison linéaire sur les q_j on se rend compte qu'ils sont liés ce qui est absurde.

■

6.1.2 Mise en oeuvre algorithmique

De cette proposition, on déduit directement l'algorithme suivant qui teste si une matrice génératrice, M, engendre un code module et trouve, dans ce cas, le polynôme générateur.

1. On transforme les lignes de la matrice M en polynômes $q_1, ..., q_{n-r}$.
2. On calcule le pgcd à droite des q_i, notons le g.
3. Si le pgcd n'est pas de degré r, le code ne peut pas provenir d'un code module.
4. Si le pgcd est de degré r, on regarde si $g, Xg, ..., X^{n-r-1}g$ sont dans le code, si oui c'est un code module engendré par g, sinon ce n'est pas un code module puisque g était le seul candidat possible.

Le calcul du pgcd est rapide grâce à l'algorithme d'Euclide.

L'algorithme ci-dessus va maintenant nous servir dans les résultats empiriques qui suivent.

6.1.3 Résultats empiriques

Voyons quelques résultats concernant les codes modules sur le corps $\mathbb{F}_2$, c'est-à-dire en commutatif.

Le tableau qui suit est à lire de la façon suivante : en colonne la longueur n du code, en ligne le polynôme générateur. Les deux chiffres se trouvant dans une case du tableau sont le cardinal des automorphismes monomiaux laissant fixe le code module et le cardinal des automorphismes monomiaux envoyant le code module sur un autre code module (y compris lui même éventuellement). Le nombre total des automorphismes monomiaux est $n!$.

Remarquons que le second nombre est un multiple du premier. En effet soit $\mathcal{C}$ un code module engendré par g et $Aut(\mathcal{C})$ le groupe des automorphismes monomiaux qui préservent ce code. S'il existe un automorphisme monomial ϕ qui envoie le code module $\mathcal{C}$ sur un autre code module $\hat{\mathcal{C}}$ alors pour tout ψ de $Aut(\mathcal{C})$, on a $\phi \circ \psi$ qui envoie également $\mathcal{C}$ sur $\hat{\mathcal{C}}$. Donc le quotient du second nombre du tableau par le premier nombre correspond au cardinal des codes modules atteints via un automorphisme monomial.

De plus $Aut(\hat{\mathcal{C}}) = \phi Aut(\mathcal{C})\phi^{-1}$.

Avec exactement le même raisonnement, nous voyons que le nombre de codes correcteurs atteints à partir d'un code module est $\frac{n!}{\sharp Aut(\mathcal{C})}$.

Deg 1	3	4	5	6	7
X	$2, 2$	$6, 6$	$24, 24$	$120, 120$	
$X+1$	$6, 6$	$24, 24$	$120, 120$	$720, 720$	
Deg 2					
X^2		$4, 4$	$12, 12$	$48, 48$	$240, 240$
X^2+1		$8, 8$	$12, 12$	$72, 72$	$144, 144$
X^2+X		$6, 6$	$24, 24$	$120, 120$	$720, 720$
X^2+X+1		$4, 4$	$8, 8$	$48, 48$	$48, 48$
Deg 3					
X^3			$12, 12$	$36, 36$	$144, 144$
X^3+1			$8, 16$	$48, 48$	$48, 48$
X^3+X			$8, 16$	$12, 12$	$72, 72$
X^3+X+1			$8, 16$	$24, 48$	$168, 336$
X^3+X^2			$12, 12$	$48, 48$	$240, 240$
X^3+X^2+1			$8, 16$	$24, 48$	$168, 336$
X^3+X^2+X			$4, 4$	$8, 8$	$48, 48$
X^3+X^2+X+1			$12, 12$	$16, 16$	$48, 48$
Deg 4					
X^4				$48, 48$	$144, 144$
X^4+1				$16, 48$	$48, 96$
X^4+X				$16, 48$	$48, 96$
X^4+X+1				$8, 32$	$8, 16$
X^4+X^2				$16, 48$	$24, 24$
X^4+X^2+1				$72, 72$	$24, 24$
X^4+X^2+X				$8, 32$	$24, 48$
X^4+X^2+X+1				$48, 144$	$168, 336$
X^4+X^3				$36, 36$	$144, 144$
X^4+X^3+1				$8, 32$	$8, 16$
X^4+X^3+X				$8, 32$	$24, 48$
X^4+X^3+X+1				$48, 144$	$16, 16$
$X^4+X^3+X^2$				$8, 8$	$16, 16$
$X^4+X^3+X^2+1$				$48, 144$	$168, 336$
$X^4+X^3+X^2+X$				$12, 12$	$16, 16$
$X^4+X^3+X^2+X+1$				$48, 48$	$48, 48$

Il est relativement peu fréquent qu'un automorphisme monomial envoie un code module sur un autre code module.

Une des questions qui reste ouverte est de prévoir quand cela va être le cas au vu du polynôme générateur g.

Une autre question intéressante est de comprendre la structure des classes d'isométries des codes modules. Voilà à titre d'exemples les polynômes de degré 4 de $\mathbb{F}_2[X]$ regroupés par **classes d'isométries**, c'est-à-dire que deux polynômes sont dans la même classe si les

codes modules qu'ils engendrent sont équivalents via un automorphisme monomial. Ici la longueur du code n vaut 6, les paramètres du code sont inscrits devant :

$$[6,2,1] : X^4$$
$$[6,2,2] : X^4+1,\ X^4+X,\ X^4+X^2$$
$$[6,2,3] : X^4+X+1,\ X^4+X^2+X,\ X^4+X^3+1,\ X^4+X^3+X$$
$$[6,2,3] : X^4+X^2+1$$
$$[6,2,4] : X^4+X^2+X+1,\ X^4+X^3+X+1,\ X^4+X^3+X^2+1$$
$$[6,2,2] : X^4+X^3$$
$$[6,2,2] : X^4+X^3+X^2$$
$$[6,2,2] : X^4+X^3+X^2+X$$
$$[6,2,2] : X^4+X^3+X^2+X+1$$

Un enjeu serait de comprendre et de prévoir ces ensembles de polynômes équivalents.

6.2 Variations autour de la non-commutativité

Il est possible d'envisager de créer des codes correcteurs à base d'anneaux polynomiaux multivariés non-commutatifs mais en changeant la forme de non-commutativité. L'essentiel pour manipuler aisément les codes correcteurs ainsi que leurs paramètres est d'avoir à nouveau un équivalent de l'algorithme de Buchberger, c'est-à-dire essentiellement de pouvoir simplifier entre eux les termes de tête de deux polynômes.

Il y a plusieurs formes de non-commutativité qui peuvent être explorées, on se place sur $\mathbb{F}_q[X,Y]$ dans ces exemples mais une généralisation peut être aisément faite.

1. Soit θ_X, $\hat{\theta}_X$, θ_Y et $\hat{\theta}_Y$ des automorphismes de $\mathbb{F}_q$, on définit la multiplication par les règles suivantes :
$$Xa = \theta_X(a)X + \hat{\theta}_X(a)Y$$
$$Ya = \theta_Y(a)Y + \hat{\theta}_Y(a)X.$$

2. On peut également introduire des dérivations, c'est-à-dire que :
$$Xa = \theta_X(a)X + \delta_X(a)$$
$$Ya = \theta_Y(a)Y + \delta_Y(a).$$

3. Il est également possible d'envisager de ne pas faire commuter les variables X et Y dans ce cas l'adaptation de l'algorithme de Buchberger semble être beaucoup plus délicate. Par exemple, on peut poser :
$$XY = YX + 1.$$

4. Enfin on peut songer à itérer la construction de Ore, c'est-à-dire de voir $\mathbb{F}_q[X,Y]$ comme étant $\mathbb{F}_q[X][Y]$. On aurait alors des relations de non-commutativité de la forme :
$$YX = \psi(X)Y + \phi(X)$$
où ψ et ϕ sont des applications de $\mathbb{F}_q[X,\theta,\delta]$.

Nous allons développer un peu le dernier exemple dans la suite de ce paragraphe.

Posons $A = \mathbb{F}_q[X,\theta]$ et trouvons les automorphismes de A. Soit ϕ un automorphisme de A. Pour des raisons de degré nous devons avoir $\phi(X) = \alpha X + \beta$ et ϕ restreint à $\mathbb{F}_q$ est un automorphisme de $\mathbb{F}_q$.

Nous avons :
$$\phi(Xa) = \phi(X)\phi(a) = (\alpha X + \beta)\phi(a) = \alpha\theta(\phi(a))X + \beta\phi(a)$$
et d'autre part :
$$\phi(Xa) = \phi(\theta(a)X) = \phi(\theta(a))(\alpha X + \beta) = \phi(\theta(a))\alpha X + \beta\phi(\theta(a))$$

Donc si $\theta = Id$, on peut prendre α et β comme l'on veut. Si $\theta \neq Id$ on doit prendre $\beta = 0$.

En résumé :

Proposition 6.2.1. — *Les automorphismes de $\mathbb{F}_q[X,\theta]$ sont donnés par, si $\theta = Id$:*
$$\begin{array}{rccc} \phi_{\alpha,\beta,\tau} & : & \mathbb{F}_q[X,\theta] & \longrightarrow & \mathbb{F}_q[X,\theta] \\ & & a & \mapsto & \tau(a) \\ & & X & \mapsto & \alpha X + \beta \end{array}$$
où $\alpha \in \mathbb{F}_q^*$, $\beta \in \mathbb{F}_q$ et $\tau \in Aut(\mathbb{F}_q)$ et si $\theta \neq Id$:
$$\begin{array}{rccc} \phi_{\alpha,\tau} & : & \mathbb{F}_q[X,\theta] & \longrightarrow & \mathbb{F}_q[X,\theta] \\ & & a & \mapsto & \tau(a) \\ & & X & \mapsto & \alpha X \end{array}$$

Grâce à la proposition précédente, il est possible de construire et de travailler dans l'anneau de Ore itéré : $\mathbb{F}_q[X,\theta][Y,\phi]$.

Remarque 6.2.2. — Il est envisageable d'ajouter des dérivations à tous les niveaux mais cela complique bien sûr un peu plus les calculs.

6.3 Codes de Goppa tordus

Les **codes de Goppa** peuvent être vus comme une généralisation des codes BCH. Ils ont des propriétés agréables puisque l'on peut contrôler leurs paramètres notamment la distance minimale. Ils possèdent un algorithme de décodage simple et ils sont bons asymptotiquement, en effet il existe une suite de codes de Goppa qui atteignent la borne de Gilbert. Pour plus de détails sur ces codes et leur construction, on pourra consulter [32].

Cette famille de codes étant construite à l'aide d'outils polynomiaux, on peut légitimement envisager une adaptation au cadre non-commutatif.

6.3.1 Définition

Définition 6.3.1. — *Soit g un polynôme de degré t à coeffcients dans $\mathbb{F}_{q^m}[X,\theta]$ et soit $L = \{\gamma_0, ..., \gamma_{n-1}\} \subset \mathbb{F}_{q^m}$ où $|L| = n$. On suppose que $X - \gamma_i$ ne divise pas à droite g, ceci pour tout $0 \leq i \leq n-1$.On pose alors $\Gamma_q^\theta(L, g)$ l'ensemble des mots $(c_0, ..., c_{n-1}) \in (\mathbb{F}_q)^n$ tels que :*

$$\sum_{i=0}^{n-1} \frac{c_i}{X - \gamma_i} \equiv 0 \ [g]_d. \tag{6.1}$$

C'est-à-dire que l'on demande que $\sum_{i=0}^{n-1} \frac{c_i}{X-\gamma_i}$ soit divisible à droite par g.

Le sens que l'on donne à $\frac{1}{X-\gamma}$ est le suivant : c'est l'unique polynôme modulo g tel que $\frac{1}{X-\gamma}(X-\gamma) \equiv 1 \ [g]_d$. Un tel polynôme existe bien, en effet si l'on effectue la division euclidienne à droite de g par $X - \gamma$, on a :

$$g = Q(X - \gamma) + c$$

où c est une constante non nulle, puisque par hypothèse $X - \gamma$ ne divise pas g à droite. On a :

$$c^{-1}g = c^{-1}Q(X - \gamma) + 1.$$

On a donc $\frac{1}{X-\gamma} = c^{-1}Q$.

On remarque également que le code $\mathcal{C}$ ainsi formé est linéaire, cependant il n'est plus forcément cyclique. Dans le cas des codes de Goppa classiques, on peut donner facilement une matrice de parité à partir des coefficients de $\frac{1}{X-\gamma_i}$. On va adapter cela au cas non-commutatif.

6.3.2 Détermination de la constante

Si l'on passe aux opérateurs aux différences associés, on a :

$$L_g(y) = L_{q_i}(\theta(y) - \gamma_i y) + c_i y.$$

Soit α_i tel que $\gamma_i = \frac{\theta(\alpha_i)}{\alpha_i}$, éventuellement α_i est dans une extension. Si l'on évalue l'égalité précédente en α_i, on obtient :

$$L_g(\alpha_i) = c_i \alpha_i.$$

C'est-à-dire :

$$c_i = \frac{L_g(\alpha_i)}{\alpha_i}.$$

D'après la définition du code de Goppa tordu une matrice de parité est formée des coefficients des polynômes $\frac{1}{X-\gamma_i}$ qui vaut $-r_i^{-1}q_i$. Il s'agit donc de trouver les coefficients de q_i pour avoir automatiquement la matrice de parité voulue.

6.3.3 Matrice de parité

Soit $g = \sum_{k=0}^{t} g_k X^k$ et soit $q_i = \sum_{k=0}^{N} q_{k,i} X^k$ où N est à déterminer.

On a :

$$g = q_i(X - \gamma_i) + c_i$$

donc

$$g - c_i = (\sum_{k=0}^{N} q_{k,i} X^k)(X - \gamma_i)$$

$$g - c_i = \sum_{k=0}^{N} q_{k,i} X^{k+1} - \sum_{k=0}^{N} q_{i,k} \theta^k(\gamma_i) X^k$$

$$g - c_i = \sum_{k=1}^{N+1} q_{k-1,i} X^k - \sum_{k=0}^{N} q_{i,k} \theta^k(\gamma_i) X^k$$

$$g - c_i = q_{N,i} X^{N+1} + \sum_{k=1}^{N} (q_{k-1,i} - q_{k,i} \theta^k(\gamma_i)) X^k - q_0 \gamma_i.$$

A présent, on peut identifier les coefficients de proche en proche en commençant par celui de plus haut degré , déjà $N = t - 1$ et

$$q_{t-1,i} = g_t$$

$$q_{t-2,i} = g_{t-1} + g_t \theta^{t-1}(\gamma_i)$$

$$q_{t-3,i} = g_{t-2} + g_{t-1} \theta^{t-2}(\gamma_i) + g_t \theta^{t-1}(\gamma_i) \theta^{t-2}(\gamma_i)$$

$$\ldots$$

$$q_{t-p,i} = \sum_{j=1}^{p} g_{t-p+j} \prod_{r=0}^{j-1} \theta^{t-p+j-1}(\gamma_i).$$

Ainsi on peut former la matrice de parité dont le terme général est

$$c_j^{-1} q_{t-i,j}.$$

Cependant dans ce cadre là, il n'est pas clair que la distance minimale soit prescrite et l'étude reste à faire.

L'adaptation très générale des codes de Goppa dans le cadre des variétés sur $\mathbb{F}_q$ reste à faire dans le cadre non-commutatif.

6.4 Codes tordus quasi-cycliques

Les codes quasi-cycliques sont une généralisation des codes cycliques. En reprenant les notations du paragraphe 2.1, c'est-à-dire en notant τ le décalage circulaire, nous avons la définition suivante :

Définition 6.4.1. — *Soit $n = lm$, un **code l-quasi-cyclique** est sous-espace vectoriel de $\mathbb{F}_q^n$ stable par τ^l.*

Définition 6.4.2. — *Un code **tordu quasi-cyclique** est un code $\mathcal{C}$ de $\mathbb{F}_q^{ml}$ vérifiant :*

$$(a_1, ..., a_l, a_{l+1}, ...a_{2l}, ...a_{ml}) \in \mathcal{C}$$

$$\Longrightarrow$$

$$(\theta(a_{(m-1)l+1}), ..., \theta(a_{ml}), \theta(a_1), ..., \theta(a_l), ..., \theta(a(m-1)l)) \in \mathcal{C}$$

Théorème 6.4.3. — *Il y a une correspondance entre les codes tordus quasi-cycliques de longueur $n = ml$ et les idéaux de $(\mathbb{F}_q[X, \theta]/\langle X^m - 1\rangle)^l$ vus comme sous $\mathbb{F}_q[X, \theta]/\langle X^m - 1\rangle$ module à gauche.*

La démonstration se fait de manière très similaire au cas θ-cyclique en calculant l'effet de la multiplication à gauche par X sur un mot de code.

L'étude de ces codes et de leurs paramètres reste à faire.

Chapitre 7

Annexe

Ces annexes présentent des tableaux de résultats concernant les codes-modules. La construction de ces tableaux est présentée au paragraphe 3 du chapitre 4, à la page 88. En ligne nous avons la longueur du code et en colonne le degré du polynôme générateur. A l'intersection d'une ligne et d'une colonne se trouve la meilleure distance minimale obtenue pour ces paramètres.

7.1 Codes-modules sur $\mathbb{F}_2[X]$

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3	3																		
4	2	4																	
5	2	3	5																
6	2	3	4	6															
7	2	3	4	4	7														
8	2	2	3	4	5	8													
9	2	2	3	4	4	6	9												
10	2	2	3	4	4	5	6	10											
11	2	2	3	4	4	5	6	7	11										
12	2	2	3	4	4	4	6	6	8	12									
13	2	2	3	4	4	4	5	6	7	8	13								
14	2	2	3	4	4	4	5	6	7	8	9	14							
15	2	2	3	4	4	4	5	6	7	8	8	10	15						
16	2	2	2	3	4	4	5	6	6	7	8	8	10	16					
17	2	2	2	3	4	4	5	6	6	7	8	8	9	11	15				
18	2	2	2	3	4	4	4	5	6	7	8	8	8	10	12	16			
19	2	2	2	3	4	4	4	5	6	7	8	8	8	9	10	12	17		
20	2	2	2	3	4	4	4	5	6	7	8	8	8	9	10	11	13	18	
21	2	2	2	3	4	4	4	5	6	7	8	8	8	8	10	10	12	14	19
22	2	2	2	3	4	4	4	5	6	7	8	8	8	8	9	10	11	12	14
23	2	2	2	3	4	4	4	4	5	7	7	8	8	8	8	10	11	12	12
24	2	2	2	3	4	4	4	4	5	6	7	8	8	8	8	9	10	11	12
25	2	2	2	3	4	4	4	4	5	6	6	7	8	8	8	8	10	10	12
26	2	2	2	3	4	4	4	4	5	6	6	6	7	8	8	8	10	10	12
27	2	2	2	3	4	4	4	4	5	6	6	6	7	8	8	8	9	10	12
28	2	2	2	3	4	4	4	4	5	6	6	6	6	7	8	8	9	10	10
29	2	2	2	3	4	4	4	4	5	6	6	6	6	7	8	8	8	9	10
30	2	2	2	3	4	4	4	4	5	6	6	6	6	6	8	8	8	9	10
31	2	2	2	3	4	4	4	4	5	6	6	6	6	7	8	8	8	9	11
32	2	2	2	2	3	4	4	4	4	6	6	6	6	6	7	8	8	8	10
33	2	2	2	2	3	4	4	4	4	6	6	6	6	6	7	8	8	8	9
34	2	2	2	2	3	4	4	4	4	5	6	6	6	6	7	8	8	8	9
35	2	2	2	2	3	4	4	4	4	5	6	6	6	6	6	8	8	8	9
36	2	2	2	2	3	4	4	4	4	5	6	6	6	6	6	7	8	8	8
37	2	2	2	2	3	4	4	4	4	5	6	6	6	6	6	7	8	8	8
38	2	2	2	2	3	4	4	4	4	4	6	6	6	6	6	7	8	8	8
39	2	2	2	2	3	4	4	4	4	4	6	6	6	6	6	7	8	8	8
40	2	2	2	2	3	4	4	4	4	4	5	6	6	6	6	7	8	8	9
41	2	2	2	2	3	4	4	4	4	4	5	6	6	6	6	7	8	8	8
42	2	2	2	2	3	4	4	4	4	4	5	6	6	6	6	7	8	8	8
43	2	2	2	2	3	4	4	4	4	4	5	6	6	6	6	7	7	8	8
44	2	2	2	2	3	4	4	4	4	4	5	6	6	6	6	7	8	8	8
45	2	2	2	2	3	4	4	4	4	4	5	6	6	6	6	6	7	8	8
46	2	2	2	2	3	4	4	4	4	4	5	6	6	6	6	6	8	8	8
47	2	2	2	2	3	4	4	4	4	4	5	6	6	6	6	6	7	8	8
48	2	2	2	2	3	4	4	4	4	4	5	6	6	6	6	6	7	8	8
49	2	2	2	2	3	4	4	4	4	4	5	6	6	6	6	6	7	8	8
50	2	2	2	2	3	4	4	4	4	4	5	6	6	6	6	6	7	8	8

	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
22	19														
23	15	21													
24	13	16	21												
25	12	14	16	22											
26	12	13	14	17	22										
27	12	13	14	15	18	24									
28	12	12	14	14	16	18	25								
29	11	12	12	14	15	16	19	24							
30	10	11	12	12	15	16	16	20	24						
31	10	12	12	12	13	16	16	17	20	25					
32	10	11	12	12	12	14	15	16	18	20	25				
33	10	10	11	12	12	13	14	16	16	18	22	28			
34	10	10	10	12	12	13	14	15	16	17	19	22	27		
35	10	10	10	12	12	12	13	14	16	16	18	20	22	28	
36	9	10	10	10	12	12	13	14	14	16	17	18	20	24	29
37	8	10	10	10	11	12	12	14	15	16	16	18	18	20	24
38	9	10	10	10	11	12	12	13	14	15	16	16	18	20	21
39	8	9	10	10	10	12	12	12	14	14	15	16	17	19	20
40	8	9	10	10	10	12	12	12	13	14	14	16	16	18	19
41	8	9	10	10	10	11	12	12	12	14	14	16	16	17	18
42	8	8	10	10	10	10	12	12	12	13	14	15	16	16	18
43	8	8	9	10	10	10	11	12	12	12	14	15	15	16	16
44	8	8	9	10	10	10	11	12	12	12	14	14	14	16	16
45	8	8	9	10	10	10	10	12	12	12	13	14	14	16	16
46	8	8	9	10	10	10	10	11	12	12	13	14	14	14	16
47	8	8	8	10	10	10	10	11	12	12	12	14	14	14	15
48	8	8	8	9	10	10	10	11	12	12	12	13	14	14	16
49	8	8	8	9	10	10	10	10	11	12	12	12	14	14	14
50	8	8	8	9	10	10	10	10	11	12	12	12	13	14	14

	36	37	38	39	40	41	42	43	44	45	46	47	48	49
37	30													
38	24	30												
39	22	25	31											
40	20	22	26	31										
41	20	20	23	26	32									
42	18	20	21	24	27	33								
43	18	20	20	22	24	27	33							
44	17	18	20	21	23	24	28	36						
45	16	18	18	20	22	24	24	28	35					
46	16	17	18	20	20	22	24	26	29	36				
47	16	16	18	18	20	21	22	24	26	30	38			
48	16	16	17	18	20	20	22	23	24	27	30	36		
49	16	16	16	18	18	20	20	22	24	24	28	31	38	
50	15	16	16	17	18	18	20	21	22	24	26	28	32	38

7.2 Codes-modules commutatifs sur $\mathbb{F}_4[X]$

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3	3																		
4	3	4																	
5	3	4	5																
6	2	3	4	6															
7	2	3	4	5	7														
8	2	3	4	5	6	8													
9	2	3	4	5	6	7	9												
10	2	3	4	5	6	6	8	10											
11	2	3	4	5	6	6	7	8	11										
12	2	3	4	4	5	6	7	8	9	12									
13	2	3	4	4	5	6	7	8	9	10	13								
14	2	3	4	4	5	6	7	7	8	10	11	14							
15	2	3	4	4	5	6	7	7	8	9	11	12	15						
16	2	3	4	4	5	6	7	7	8	9	10	12	12	16					
17	2	3	4	4	5	5	7	7	7	8	9	10	12	13	17				
18	2	3	3	4	4	5	6	7	7	8	9	10	11	13	14	18			
19	2	3	3	4	5	5	6	6	7	8	9	10	11	12	14	15	19		
20	2	3	3	4	5	5	6	6	7	8	8	9	10	11	12	14	16	20	
21	2	3	3	4	5	5	6	6	7	7	8	9	10	11	12	13	15	16	21
22	2	2	3	4	4	5	5	6	7	7	8	9	10	10	11	13	14	15	17
23	2	2	3	4	4	5	5	6	6	7	8	9	9	10	11	12	13	15	16
24	2	2	3	4	4	5	5	6	6	7	8	8	9	10	11	12	13	14	16
25	2	2	3	4	4	5	5	6	6	7	8	8	9	10	10	11	12	13	14
26	2	2	3	4	4	5	5	6	6	7	7	8	9	10	10	11	12	13	14
27	2	2	3	4	4	5	5	6	6	7	7	8	9	9	10	11	12	13	14
28	2	2	3	4	4	5	5	6	6	7	7	8	8	9	10	11	11	12	13
29	2	2	3	4	4	5	5	6	6	7	7	8	8	9	10	10	11	12	13
30	2	2	3	4	4	5	5	6	6	7	7	8	8	9	10	10	11	12	12
31	2	2	3	4	4	5	5	5	6	7	7	8	8	9	10	10	11	11	12
32	2	2	3	4	4	5	5	6	6	6	7	8	8	9	9	10	11	11	12
33	2	2	3	4	4	5	5	6	6	6	7	7	8	9	9	10	10	11	12
34	2	2	3	4	4	5	5	5	6	6	7	7	8	8	9	10	10	11	12
35	2	2	3	4	4	5	5	6	6	6	7	7	8	8	9	10	10	11	12
36	2	2	3	3	4	5	5	5	6	6	7	7	8	8	9	9	10	11	11
37	2	2	3	3	4	5	5	6	6	6	7	7	8	8	9	9	10	10	11
38	2	2	3	3	4	5	5	5	6	6	7	7	8	8	9	9	10	10	11
39	2	2	3	3	4	5	5	6	6	6	7	7	7	8	9	9	10	10	11
40	2	2	3	3	4	5	5	6	6	6	6	7	8	8	8	9	10	10	11

	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
22	22																		
23	18	23																	
24	17	19	24																
25	16	18	20	24															
26	16	17	19	20	26														
27	15	16	18	19	21	27													
28	14	15	17	18	20	22	28												
29	14	15	16	17	19	21	23	29											
30	13	14	16	17	18	19	21	24	30										
31	13	14	15	16	17	19	20	22	24	30									
32	13	14	15	16	17	18	19	21	23	25	32								
33	13	13	14	15	16	17	18	20	22	24	26	33							
34	12	13	14	15	16	17	18	19	21	22	25	27	33						
35	12	13	14	15	15	16	18	19	20	21	23	25	28	34					
36	12	13	14	14	15	16	17	18	19	21	22	24	26	28	35				
37	12	13	13	14	15	16	17	18	19	20	21	23	25	27	29	36			
38	12	12	13	14	15	16	16	17	19	19	21	22	24	25	27	30	37		
39	12	12	13	14	14	15	16	17	18	19	20	21	22	24	26	28	31	37	
40	11	12	13	13	14	15	16	17	18	19	20	21	22	23	25	27	29	32	39

7.3 Codes-modules sur $\mathbb{F}_4[X, \theta]$

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3	3																		
4	3	4																	
5	2	4	5																
6	2	4	4	6															
7	2	3	4	5	7														
8	2	3	4	5	6	8													
9	2	3	4	5	6	7	9												
10	2	3	4	5	6	6	8	10											
11	2	3	4	4	6	6	7	8	11										
12	2	3	4	4	6	6	7	8	9	12									
13	2	3	4	4	5	6	7	8	9	10	13								
14	2	3	4	4	5	6	7	7	8	10	11	14							
15	2	2	3	4	5	5	6	8	8	9	11	12	15						
16	2	2	3	4	4	5	6	7	8	9	10	11	12	16					
17	2	2	3	4	4	5	6	7	7	8	9	10	12	13	17				
18	2	2	3	4	4	5	6	7	7	8	9	10	11	13	14	18			
19	2	2	3	4	4	5	6	7	8	8	9	10	11	12	13	15	19		
20	2	2	3	4	4	5	6	7	7	8	8	9	10	11	13	14	16	20	
21	2	2	3	4	4	5	5	6	7	8	9	9	10	11	12	13	15	16	21
22	2	2	3	4	4	5	5	6	7	8	8	9	10	11	12	13	14	16	17
23	2	2	3	4	4	4	5	6	7	7	8	9	9	10	11	12	13	15	16
24	2	2	3	4	4	4	5	6	6	7	8	8	9	10	11	12	13	14	15
25	2	2	3	4	4	4	5	6	6	7	8	8	9	10	10	11	12	13	15
26	2	2	3	4	4	4	5	6	6	7	8	8	9	10	10	11	12	13	14
27	2	2	3	4	4	4	5	6	6	7	7	8	9	9	10	11	12	13	14
28	2	2	3	4	4	4	5	6	6	7	8	8	9	9	10	11	11	12	13
29	2	2	3	4	4	4	5	6	6	7	7	8	8	9	10	11	11	12	13
30	2	2	3	4	4	4	5	6	6	7	7	8	8	9	10	10	11	12	13
31	2	2	2	3	4	4	5	6	6	6	7	8	8	9	9	10	11	12	12
32	2	2	2	3	4	4	5	6	6	6	7	8	8	9	9	10	11	12	12
33	2	2	2	3	4	4	5	6	6	6	7	7	8	8	9	10	10	11	12
34	2	2	2	3	4	4	5	6	6	6	7	7	8	8	9	10	10	11	12
35	2	2	2	3	4	4	4	5	6	6	6	7	8	8	9	10	10	11	12
36	2	2	2	3	4	4	4	5	6	6	7	7	8	8	9	9	10	11	11
37	2	2	2	3	4	4	4	5	6	6	7	7	8	8	9	9	10	11	11
38	2	2	2	3	4	4	4	5	6	6	7	7	8	8	9	9	10	10	11
39	2	2	2	3	4	4	4	5	6	6	7	7	7	8	8	9	10	10	11
40	2	2	2	3	4	4	4	5	6	6	7	7	8	8	9	9	10	10	11

	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
22	22																		
23	8	23																	
24	17	19	24																
25	16	18	20	25															
26	15	17	19	20	26														
27	15	16	17	20	21	27													
28	14	15	17	18	20	22	28												
29	14	15	16	17	19	21	23	29											
30	14	15	16	17	18	20	21	24	30										
31	13	14	15	16	17	19	20	23	24	31									
32	13	14	15	16	17	18	19	21	23	25	31								
33	13	14	14	15	16	17	19	20	22	24	26	33							
34	12	13	14	15	16	17	18	20	21	22	24	27	34						
35	12	13	14	15	16	16	18	19	20	21	23	25	28	35					
36	12	13	14	14	15	16	17	18	20	21	22	24	26	28	36				
37	12	13	13	14	15	16	17	18	19	20	21	23	25	27	29	36			
38	12	12	13	14	15	16	16	17	18	19	21	22	24	25	28	30	37		
39	12	12	13	14	14	15	16	17	18	19	20	21	23	24	26	28	31	38	
40	11	12	13	13	14	15	16	17	18	19	20	21	22	23	25	27	29	32	39

7.4 Codes-modules sur $\mathbb{F}_4[X, \theta, \delta_1]$

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3	3																		
4	3	4																	
5	3	4	5																
6	2	3	4	6															
7	2	3	4	5	7														
8	2	3	4	5	6	8													
9	2	3	4	5	6	7	9												
10	2	3	4	4	5	6	8	10											
11	2	3	3	4	5	6	7	8	11										
12	2	3	3	4	5	6	7	8	9	12									
13	2	3	3	4	5	6	6	8	9	10	13								
14	2	3	3	4	5	6	6	7	8	10	11	14							
15	2	3	3	4	4	6	6	7	8	9	10	12	15						
16	2	2	3	4	4	5	6	7	7	8	10	11	12	16					
17	2	2	3	4	4	5	6	6	7	8	9	10	12	13	17				
18	2	2	3	4	4	5	6	6	7	8	9	10	11	12	14	18			
19	2	2	3	3	4	5	6	6	7	7	8	9	10	12	13	15	19		
20	2	2	3	3	4	5	6	6	6	7	8	9	10	11	12	14	16	20	
21	2	2	3	3	4	5	6	6	6	7	8	9	9	11	12	13	15	16	21
22	2	2	3	3	4	5	5	6	6	7	8	8	9	10	11	12	14	15	17
23	2	2	3	3	4	4	5	6	6	7	7	8	9	10	11	12	13	15	16
24	2	2	3	3	4	4	5	6	6	7	7	8	9	10	10	11	13	14	15
25	2	2	3	3	4	4	5	6	6	6	7	8	8	9	10	11	12	13	14
26	2	2	3	3	4	4	5	6	6	6	7	8	8	9	10	11	11	12	14
27	2	2	3	3	4	4	5	6	6	6	7	7	8	9	10	10	11	12	13
28	2	2	3	3	4	4	5	6	6	6	7	7	8	9	9	10	11	12	13
29	2	2	3	3	4	4	5	6	6	6	7	7	8	8	9	10	11	12	13
30	2	2	3	3	4	4	5	5	6	6	6	7	8	8	9	10	10	11	12
31	2	2	3	3	4	4	5	5	6	6	6	7	8	8	9	10	10	11	12
32	2	2	3	3	4	4	5	5	6	6	6	7	8	8	9	9	10	11	12
33	2	2	3	3	4	4	4	5	5	6	6	7	7	8	9	9	10	11	11
34	2	2	3	3	4	4	4	5	6	6	6	7	7	8	8	9	10	10	11
35	2	2	3	3	4	4	4	5	5	6	6	7	7	8	8	9	10	10	11
36	2	2	3	3	4	4	4	5	6	6	6	7	7	8	8	9	10	10	11
37	2	2	3	3	4	4	4	5	5	6	6	7	7	8	8	9	9	10	11
38	2	2	3	3	3	4	4	5	5	6	6	7	7	7	8	9	9	10	10
39	2	2	3	3	3	4	4	5	5	6	6	6	7	7	8	9	9	10	10
40	2	2	3	3	3	4	4	5	5	6	6	6	7	7	8	8	9	10	10

	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
22	22																		
23	18	23																	
24	17	19	24																
25	16	18	20	25															
26	15	17	18	20	26														
27	14	16	17	19	21	27													
28	14	15	16	18	20	22	28												
29	13	15	16	17	19	21	23	29											
30	13	14	15	16	18	20	21	24	29										
31	13	14	15	16	17	18	20	22	24	31									
32	13	13	14	15	16	18	19	21	23	25	32								
33	12	13	14	15	16	17	18	20	22	24	26	32							
34	12	13	14	15	15	16	18	19	20	22	24	27	34						
35	12	12	13	14	15	16	17	18	19	21	23	25	28	34					
36	12	12	13	14	15	16	17	18	19	20	22	24	25	28	35				
37	11	12	13	14	14	16	16	17	18	20	21	23	24	27	29	37			
38	11	12	13	14	14	15	16	17	18	19	20	22	23	25	27	30	37		
39	11	12	12	13	14	15	16	17	17	19	20	21	22	24	26	28	31	38	
40	11	12	12	13	14	14	15	16	17	18	19	20	22	23	25	26	29	32	39

7.5 Codes-modules sur $\mathbb{F}_4[X, \theta, \delta_2]$

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3	3																		
4	2	4																	
5	2	3	5																
6	2	3	4	6															
7	2	3	4	5	7														
8	2	3	4	5	6	8													
9	2	3	4	5	6	7	9												
10	2	3	4	5	6	6	8	10											
11	2	3	4	4	5	6	7	8	11										
12	2	3	4	4	5	6	7	8	9	12									
13	2	3	4	4	5	6	6	7	9	10	13								
14	2	3	4	4	5	6	6	7	8	10	11	14							
15	2	2	3	4	5	5	6	7	8	9	10	12	15						
16	2	2	3	4	5	5	6	7	8	8	10	11	12	16					
17	2	2	3	4	4	5	6	7	7	8	9	10	12	13	17				
18	2	2	3	4	4	5	6	7	7	8	9	10	11	12	14	18			
19	2	2	3	4	4	5	6	6	7	8	9	9	10	12	13	15	19		
20	2	2	3	4	4	5	6	6	7	7	8	9	10	11	12	14	16	20	
21	2	2	3	4	4	5	5	6	7	7	8	9	10	11	12	13	14	16	21
22	2	2	3	4	4	5	5	6	7	7	8	9	9	10	11	12	14	15	17
23	2	2	3	4	4	4	5	6	6	7	8	8	9	10	11	12	13	14	16
24	2	2	3	4	4	4	5	6	6	7	8	8	9	10	11	11	12	14	15
25	2	2	3	4	4	4	5	6	6	7	7	8	9	9	10	11	12	13	14
26	2	2	3	4	4	4	5	6	6	7	7	8	8	9	10	11	12	13	14
27	2	2	3	4	4	4	5	6	6	7	7	8	8	9	10	11	11	12	13
28	2	2	3	4	4	4	5	6	6	6	7	8	8	9	10	10	11	12	13
29	2	2	3	4	4	4	5	6	6	6	7	8	8	9	9	10	11	12	13
30	2	2	3	4	4	4	5	5	6	6	7	8	8	9	9	10	11	11	12
31	2	2	2	3	4	4	5	5	6	6	7	7	8	8	9	10	10	11	12
32	2	2	2	3	4	4	5	5	6	6	7	7	8	8	9	10	10	11	12
33	2	2	2	3	4	4	5	5	6	6	7	7	8	8	9	10	10	11	12
34	2	2	2	3	4	4	5	5	6	6	7	7	8	8	9	10	10	11	11
35	2	2	2	3	4	4	4	5	5	6	6	7	7	8	9	9	10	11	11
36	2	2	2	3	4	4	4	5	6	6	6	7	7	8	9	9	10	10	11
37	2	2	2	3	4	4	4	5	5	6	6	7	7	8	9	9	10	10	11
38	2	2	2	3	4	4	4	5	5	6	6	7	7	8	8	9	10	10	11
39	2	2	2	3	4	4	4	5	5	6	6	7	7	8	8	9	9	10	11
40	2	2	2	3	4	4	4	5	5	6	6	7	7	8	8	9	9	10	11

	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
22	22																		
23	18	23																	
24	17	19	24																
25	16	17	20	25															
26	15	16	18	20	26														
27	14	16	17	19	21	27													
28	14	15	17	18	20	22	28												
29	14	15	16	17	19	21	23	29											
30	13	14	15	16	18	19	21	24	29										
31	13	14	15	16	17	18	20	22	24	31									
32	13	14	14	15	17	18	19	21	23	25	31								
33	12	13	14	15	16	17	18	20	21	24	26	33							
34	12	13	14	15	16	17	18	19	20	22	24	27	34						
35	12	13	13	14	15	16	17	19	19	21	23	25	28	34					
36	12	12	13	14	15	16	17	18	19	20	22	23	25	28	35				
37	12	12	13	14	15	16	16	17	19	20	21	23	24	26	29	37			
38	11	12	13	14	14	15	16	17	18	19	20	22	23	25	28	30	37		
39	11	12	13	13	14	15	16	17	18	19	20	21	22	24	26	28	31	39	
40	11	12	12	13	14	15	15	17	17	18	19	20	22	23	24	26	28	32	39

Bibliographie

[1] T. Berger. Isometries for rank distance and permutation group of Gabidulin codes. *IEEE Trans.Inform.Theory*, 49(111) :3016–3019, 2003.

[2] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, and A. Wassermann. *Error-Correcting Linear Codes*. Springer, 2000.

[3] P-L. Cayrel, C.Chabot, and A.Necer. Quasi-cyclic codes as codes over rings of matrices. *Finite Fields and their Applications*, 16 :100–115, 2010.

[4] F. Chyzak and B. Salvy. Non-commutative elimination in Ore algebras proves multivariate holonomic identities. *Journal of Symbolic Computation*, 26(2) :187–227, 1998.

[5] P. M. Cohn. *Skew Fields*. Cambridge University Press, 1995.

[6] R. S. Coulter, G. Havas, and M. Henderson. On decomposition of sub-linearised polynomials. *Journal of Australian Mathematical Society*, 76 :317–328, 2004.

[7] D. A. Cox, J. B. Little, and D. O'Shea. *Ideals, Varieties and Algorithms*. Springer, 1996.

[8] D.Boucher, P.Solé, and F.Ulmer. Skew Constacyclic Codes over Galois Rings. *Advances in Mathematics of Communications*, 2 :273–292, 2008.

[9] E. M. Gabidulin. Problems of information transmission. *Russian Original*, 21, 1985.

[10] P. Gaborit and A. Otmani. Tables of Euclidian and Hermitian self-dual codes over GF(4). *http ://www. unilim. fr/pagesperso/philippe. gaborit/SD/.*

[11] M. Giesbrecht. Factoring in Skew-Polynomial Rings over Finite Fields. *Journal of Symbolic Computation*, 26 :463–486, 1998.

[12] N. Jacobson. *The Theory of Rings*. American Mathematical Society.

[13] N. Jacobson. *Finite-Dimensional Division Algebras over Fields*. Springer, 1996.

[14] R. Lidl and H. Niederreiter. *Finite Fields*. Addison-Wesley, 1996.

[15] P. Loidreau. A Welch-Berlekamp like algorithm for decoding Gabidulin codes. *Coding and Cryptography-Revised selected papers of WCC 2005, 2006*, LNCS 3969 :36–45, 2006.

[16] B. R. McDonald. *Finite Rings with Identity*. MarcelDekker Inc., 1994.

[17] R. McEliece. A public-key cryptosystem based on algebraic coding theory. *JPL DSN Progress Report*, 4244 :114–116, 1978.

[18] E. MGabidulin, GA. V. Paramonov, and O. V. Tretjakov. Ideals over a noncommutative ring and their application in cryptology. *Lecture Notes in Computer Science*, 547 :482–489, 1991.

[19] Müller. Gröbnerbasen in Ore-Algebren. *Dissertation zur Erlangung des akademischen Grades eines Doktors der Mathematik*, 2006.

[20] O. Ore. On a special class of polynomials. *Transactions of the American Mathematical Society*, 35 No 3 :559–584, 1933.

[21] O. Ore. Theory of Non-Commutative Polynomials. *The Annals of Mathematics*, 34 :480–508, 1933.

[22] O. Papini and J. Wolfmann. *Algèbre discrète et codes correcteurs*. Springer, 1995.

[23] M. Pesch. Two-sided Gröbner bases in iterated Ore extensions. *MIP-9602*, 1996.

[24] C. Rigioni. Construction of n-variables codes. *Discrete Mathematics*, 56 :275–280, 1985.

[25] R. M. Roth. Maximum-Rank array codes and their application to crisscross error correction. *IEEE Transactions on Information Theory*, 37 :328–336, 1991.

[26] N. Sendrier. On the dimension of the hull. *SIAM Journal on Discrete Mathematics*, 10 :282–293, 1997.

[27] N. Sendrier. Finding the permutation between equivalent codes : the support splitting algorithm. *IEEE Transactions on Information Theory*, 46 :1193–1203, 2000.

[28] M. F. Singer and M. Van der Put. *Galois Theory of linear differentials equations*. Springer, 2003.

[29] F. Ulmer and D. Boucher. Codes as modules over skew polynomials rings. 2009.

[30] F. Ulmer and D. Boucher. Coding with skew polynomials rings. *Journal of Symbolic Computation*, 44 :1644–1656, 2009.

[31] F. Ulmer, D. Boucher, and W. Geiselmann. Skew Cyclic Codes. *Applied Algebra in Engineering, Communication and Computing*, 18 :379–389, 2007.

[32] J. H van Lint. *Introduction to Coding Theory*. Springer-Verlag, 1991.

[33] E. Wexler-Kreindler. Sur une classification des extensions d'Öre. *C. R. Acad. Sc. Paris*, 282 série A :1331–1333, 1976.

RÉSUMÉ

Les anneaux de polynômes sont l'un des outils privilégiés pour construire et étudier des familles de codes correcteurs. Nous nous proposons, dans cette thèse, d'utiliser des anneaux de Ore, qui sont des anneaux de polynômes non-commutatifs, afin de créer des codes correcteurs.

Cette approche nous permet d'obtenir des familles de codes correcteurs plus larges que si l'on se restreint au cas commutatif mais qui conservent de nombreuses propriétés communes.

Nous obtenons notamment un algorithme qui permet de fabriquer des codes correcteurs dont la distance de Hamming ou la distance rang est prescrite. C'est ainsi que nous avons exhibé deux codes qui améliorent la meilleure distance minimale connue pour un code de même longueur et de même dimension. L'un est de paramètres $[42, 14, 21]$ sur le corps $\mathbb{F}_8$ et l'autre de paramètres $[40, 23, 10]$ sur $\mathbb{F}_4$.

La généralisation de cette étude au cas d'anneaux polynomiaux multivariés est également présentée ; l'outil principal est alors la théorie des bases de Gröbner qui s'adapte dans ce cadre non-commutatif et permet de manipuler des idéaux pour créer de nouvelles familles de codes correcteurs.

ABSTRACT

We generalize the notion of cyclic code and we construct codes as ideals in finite quotients of non-commutative polynomial rings, so called Ore rings. We propose a method to obtain block codes of prescribed rank or Hamming distance. In particular we construct a $[42, 14, 21]_8$ code by imposing a rank and a $[40, 20, 10]_4$ code by imposing a distance, which both improve by one the minimum distance of the previously best known linear codes with the same length and dimension over those fields.

We also study some multivariate Ore rings and the generalization of the Buchberger's algorithm allows us to manipulate the ideals of these rings and to build skew codes. We obtain, in particular, the generator matrix in the standard form.